

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK**

JOCELYN TROELL, individually, and for the estate of  
STEPHEN TROELL, NOOR ALKHALILI,  
individually, and for the estate of NAWRES WALEED  
HAMID, A.W. by and through his next friend Noor  
Alkhalili, H.W. by and through his next friend Noor  
Alkhalili, TONI ALEXANDER, BROCK JOHNSON,  
SHANERRIA BARBER, PATRICK BEN,  
BADEKEMI BILADJETAN, EINREB BISMANOS,  
JULIUS BRISCO, MELISSA BRISCO, T.B. by and  
through his next friend Julius Brisco, J.M. by and  
through his next friend Melissa Brisco, ALI BROWN,  
TIMOTHY BROWN, JAMES CARSON,  
MACKENZIE HARLOW, JARON CARTER, OLIVIA  
CARTER, J.C. by and through her next friend Jaron  
Carter, THOMAS CAUDILL, ADRIENNE CAUDILL,  
L.M.C. by and through his next friend Thomas Caudill,  
L.S.C. by and through his next friend Thomas Caudill,  
O.C. by and through his next friend Thomas Caudill,  
R.C. by and through her next friend Thomas Caudill,  
DOLPHISE COLOMB, M.W. by and through his next  
friend Dolphise Colomb, QUINTIN COPELAND,  
TAYANA ROMAN, NECOLLIER DANIELS,  
SARAH DANIELS, C.M.D. by and through his next  
friend Necollier Daniels, C.T.D. by and through his next  
friend Necollier Daniels, JACOB DEER, SAMANTHA  
DEER, J.A.S.D. by and through his next friend Jacob  
Deer, J.C.B.D. by and through his next friend Jacob  
Deer, COREY FAUCETT, THOMAS  
FELDSCHNEIDER, COURTNEY  
FELDSCHNEIDER, J.F. by and through his next friend  
Thomas Feldschneider, N.S. by and through his next  
friend Kimberly Starnes, JULIE FERGUSON,  
MITCHELL FERGUSON, MIGUEL FIGUEROA,  
STEVEN GARRETT, HEATHER GARRETT, S.G. by  
and through his next friend Steven Garrett, BRANDON  
GODWIN, DUSTIN GRAHAM, MALISSA  
GRAHAM, H.G. by and through her next friend Dustin  
Graham, J.G. by and through her next friend Dustin  
Graham, STEPHON GREEN, MENTORIA GREEN,  
A.G. by and through his next friend Stephon Green,  
S.G. by and through her next friend Stephon Green,  
NATHAN GROSSE, BRETT GUSTAFSON,  
AMANDA GUSTAFSON, L.G. by and through his

Case No.: 1:24-cv-7136

JURY TRIAL DEMANDED

next friend Brett Gustafson, GEOFFREY HANSEN, ALLIE HANSEN, JOHN HERGERT, ALYSSA HERGERT, C.H. by and through his next friend John Hergert, COSTIN HERWIG, JENNIFER DEAVER, J.H. by and through his next friend Costin Herwig, J.F.D. by and through his next friend Jennifer Deaver, J.X.D. by and through his next friend Jennifer Deaver, BRANDON HITCHINGS, SUZANNE HODGES, KERRY HOWARD, ANDREW JENKINS, MEGAN JENKINS, A.J. by and through her next friend Andrew Jenkins, P.J. by and through his next friend Andrew Jenkins, S.J. by and through her next friend Andrew Jenkins, ALAN JOHNSON, TERI LARSON-JOHNSON, J.J. by and through his next friend Alan Johnson, ABBY SIGURDSON, CARLY SIGURDSON, SAMUEL SIGURDSON, TREMAYNE JOINER, ROBERT JONES, DAUNTE KELLER, ALEXANDER KNOWLES, DAINE KVASAGER, C.K. by and through his next friend Daine Kvasager, R.K. by and through his next friend Daine Kvasager, REBECCA KVASAGER, L.M. by and through her next friend Rebecca Kvasager, KENNETH LEWIS, TAMMY SENECALEWIS, K.L. by and through her next friend Kenneth Lewis, R.L. by and through his next friend Kenneth Lewis, R.A.L. by and through her next friend Kenneth Lewis, TAVERA GREEN, LEIGHTON LIM, DEANNA LUCCHESI, JOSHUA LUCCHESI, A.L. by and through her next friend Deanna Lucchesi, H.L. by and through her next friend Deanna Lucchesi, Z.L. by and through her next friend Deanna Lucchesi, JOHN MAGEE, DARIUS MARTIN, AMANDA MARTIN, M.M. by and through his next friend Darius Martin, DARLINA MARTIN, CAYLEIGH MARTIN, ISAAC MARTZ, TORRIN MCDUGLE, PHILLIP MENDOZA, MELCHI MENDOZA, A.M. by and through his next friend Phillip Mendoza, ZACHARY MERRILL, CAROLINA MERRILL, C.M. by and through her next friend Zachary Merrill, JAMES MORGAN, SARAH MORGAN, C.M. by and through her next friend James Morgan, RYAN NOLAN, BRITTANY NORFLEET, ANTHONY SHAPPY, A.S. by and through her next friend Brittany Norfleet, K.S. by and through her next friend Brittany Norfleet, JOSE ORTIZ, ANTHONY PANCHOO, ALEXIS PANCHOO, A.P. by and through her next friend Anthony Panchoo, CARLOS PORRES JR., K.L.P. by

and through her next friend Carlos Porres Jr., K.R.P. by  
and through her next friend Carlos Porres Jr.,  
MICHAEL PRIDGEON, REBECCA PRIDGEON, A.P.  
by and through her next friend Michael Pridgeon, M.P.  
by and through his next friend Michael Pridgeon, T.P.  
by and through his next friend Michael Pridgeon,  
RACHEL QUINN, FRANCINE RIOS, individually,  
and for the estate of JASON QUITUGUA II,  
MCKENZIE-JAE QUITUGUA, KAEDINN  
QUITUGUA, SUMMER QUITUGUA, NILSA  
RIVERA VILLEGAS, JACOB SCHMIDT, JARON  
SCHNEIDER, ASHLEY SCHNEIDER, COLLIN  
SHEPARD, KAITLIN SHEPARD, FREDERICK  
SHILKE, STEPHANIE SHILKE, W.S. by and through  
his next friend Frederick Shilke, M.C.R. by and through  
his next friend Stephanie Shilke, M.D.R. by and through  
her next friend Stephanie Shilke, MICHAEL SMITH,  
CORISIA SMITH, A.S. by and through her next friend  
Michael Smith, A.D. by and through her next friend  
Corisia Smith, GREGORY SORENSEN, HUGH  
SPEARS JR., BRANDON SPEARS, JOHNATHAN  
STARK, WILLIAM TABER, DAGMAR TABER,  
LOUIS PALLA, SAMIRA PALLA, A.T. by and  
through her next friend William Taber, NICOLAUS  
TRIVELPIECE, SANDRO VICENTE, LUIS  
VILLEGAS, HAILEY WEBSTER, JOHN GOETZ,  
JEREMY WINKLER, TYLA WINKLER, M.A.W. by  
and through his next friend Jeremy Winkler, M.I.W. by  
and through his next friend Jeremy Winkler, M.Z.W. by  
and through her next friend Jeremy Winkler, MASON  
WRIGHT, A.V. by and through her next friend Mason  
Wright, BIANCA MEZA-COVARRUBIAS, SHIWA  
NAHADI, individually, and for the estate of OMER  
MAHMOUDZADEH, TARA MAHMOUDZADEH,  
BERNADETTE BRAUNER, NIR BRAUNER,  
SHEEREL GABAY, AMIR FAKHRAVAR, AKBAR  
LAKESTANI, KEVIN KING, STEPHANIE MILLER,  
NICOLE KAMALESON, BARCLAY KAMALESON,  
CADE KAMALESON, CEDRIC KAMALESON,  
SUNDERRAJ KAMALESON, DEANNA SARTOR,  
G.S. by and through his next friend Deanna Sartor,  
GRACE SARTOR, STRYDER SARTOR, MARY  
PRYOR-PATTERSON, JAMES SARTOR, SHAE  
SARTOR, GRACE KREISCHER, C.K. by and through  
his next friend Grace Kreischer, BRIANNE BARLOW,  
JASON BARLOW, SAGE SALADIN,

SHUSHAWNDRA GREGOIRE, JOHN GREGOIRE JR., JOHN GREGOIRE SR., L.G. by and through her next friend John Gregoire Sr., HOPE HARRISON, H.H. by and through her next friend Hope Harrison, DONNA HARRISON, MARLIN HARRISON, HEIDE RYAN, HENRY MAYFIELD SR., DANIELLE DAVIS, TALIJAH DAVIS, RONALD EDWARDS, NICHOLAS MAYFIELD, TYSHAUNA WHITE, CARMONETA HORTON-MAYFIELD, TYRON EDWARDS, CIARA MARTIN, MARK FRERICHES, CHARLENE CAKORA, MICHELLE BLACK, EZEKIEL BLACK, I.B. by and through his next friend Michelle Black, KAREN BLACK, HENRY BLACK, JASON BLACK, CRYSTAL JOHNSON, ADDIE JOHNSON, ELISA JOHNSON, JOHN JOHNSON, JENNIFER JOHNSON, JO-ANNE JOHNSON, MYESHIA JOHNSON, RICHSHAMA JOHNSON, TABITHA FARMER, individually, and for the estate of JONATHAN ROBERT FARMER, B.F. by and through her next friend Tabitha Farmer, D.F. by and through his next friend Tabitha Farmer, P.J.F. by and through his next friend Tabitha Farmer, P.F. by and through her next friend Tabitha Farmer, AMINA SHAHEEN, individually, and for the estate of GHADIR TAHER, KAWA TALABANI, SAUNDRA WIRTZ, DAVID WIRTZ, FRANCES WIRTZ, RICHARD HERRERA, MICHAEL GRETZON, RANDI GRETZON, MARK SCHMITZ, SUZANNE SCHMITZ, A.S. by and through her next friend Mark Schmitz, CAMERON SCHMITZ, E.S. by and through her next friend Mark Schmitz, JACLYN SCHMITZ, and TRAVIS AVENVILI-FRKOVIC,

Plaintiffs,

v.

BINANCE HOLDINGS LIMITED d/b/a BINANCE  
and BINANCE.COM, and CHANGPENG ZHAO,

Defendants.

**COMPLAINT FOR VIOLATIONS OF THE ANTI-TERRORISM ACT**

## **TABLE OF CONTENTS**

INTRODUCTION .....	1
THE PARTIES.....	3
JURISDICTION AND VENUE .....	8
CRYPTOCURRENCY PRIMER .....	10
FACTUAL ALLEGATIONS .....	14
I. From 2003 Through 2024, The Islamic Revolutionary Guard Corps Led A Jihadist “Axis of Resistance” Comprised Of Designated Foreign Terrorist Organizations That Partnered To Conduct Terrorist Attacks Targeting The United States.....	14
A. The Islamic Revolutionary Guards Corps.....	17
1. The IRGC Was an Integrated Global Terrorist Organization.....	17
2. The IRGC Was Purpose-Built to Attack the United States as Its Primary Mission.....	19
3. The IRGC and Supreme Leader’s Office Seized Key Iranian Economic Sectors to Finance, Arm, and Logistically Support IRGC-Sponsored Terrorist Attacks .....	41
a. The Sanctions Evasion Sector.....	43
b. The Financial Sector .....	43
c. The Import/Export Sector .....	44
d. The Communications Sector.....	46
B. Hezbollah .....	47
C. Hamas .....	49
D. Palestinian Islamic Jihad.....	50
E. Al-Qaeda.....	52
II. From 2014 Through 2024, ISIS Conducted Terrorist Attacks Targeting The United States .....	54
III. Defendants Knowingly Enabled Foreign Terrorist Organizations And Iran, The World’s Foremost State Sponsor Of Anti-American Terrorism, To Conduct Hundreds Of Millions Of Dollars Of Prohibited Terrorist Finance Transactions.....	57

IV.	Defendants Were Generally Aware That The Terrorist Attacks On Plaintiffs And Their Family Members Were A Foreseeable Consequence Of Willingly Enabling Foreign Terrorist Organizations’ Transactions On The Binance Exchange .....	69
A.	Defendants Were Generally Aware that FTOs Embraced Cryptocurrency to Fund Terrorist Attacks .....	70
1.	Warnings from the U.S. Government .....	71
2.	Warnings from the International Community .....	75
3.	Warnings from Blockchain Analysis Firms, Terrorism Scholars, and NGOs .....	77
B.	Defendants Were Generally Aware That The IRGC, Hezbollah, and Kataib Hezbollah Embraced Cryptocurrency to Fund Terrorist Attacks .....	78
1.	Warnings from the U.S. Government .....	80
2.	Warnings from Blockchain Analysis Firms.....	82
3.	Warnings from Terrorism Scholars and NGOs .....	84
C.	Defendants Were Generally Aware That Hamas and PIJ Embraced Cryptocurrency to Fund Terrorist Attacks.....	86
1.	Warnings from the U.S. Government .....	86
2.	Warnings from Blockchain Analysis Firms.....	88
D.	Defendants Were Generally Aware That Al-Qaeda and ISIS Embraced Cryptocurrency to Fund Terrorist Attacks.....	89
1.	Warnings from the U.S. Government .....	89
2.	Warnings from the United Nations .....	91
3.	Warnings From Blockchain Analysis Firms, Terrorism Scholars, and NGOs .....	92
E.	Defendants Disregarded Voluminous Warnings That Operating an Illegal Money Transmittal Business and Defying U.S. AML/CFT and KYC Rules Foreseeably Aided Attacks by the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, and ISIS.....	94
F.	Defendants Disregarded Voluminous Warnings That Processing Transactions for Customers in Violation of U.S. Counterterrorism Sanctions, Including U.S. Countrywide Sanctions, Targeting Iran, Syria, the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, or ISIS Foreseeably Aided Terrorist Attacks.....	98

V.	Defendants Knowingly Enabled Foreign Terrorist Organizations And Their Affiliates To Transact On The Binance Exchange .....	101
	A. Defendants’ Admissions .....	102
	B. Defendants’ Consciousness of Guilt .....	104
	C. Blockchain Analysis Software and Warnings from Third Parties .....	107
	D. Alternatively, Defendants Willfully Blinded Themselves to the Enormous Volume of Transactions on the Binance Exchange That Enabled FTOs To Carry Out Terrorist Attacks .....	111
VI.	Defendants Knowingly And Substantially Assisted Terrorist Attacks Committed By The IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS That Targeted The United States And Killed Or Injured Plaintiffs .....	115
	A. The IRGC’s, Hezbollah’s, and Kataib Hezbollah’s Attacks on Plaintiffs .....	129
	1. Defendants Knowingly Enabled IRGC Members, Affiliates, and Fronts to Transact on the Binance Exchange .....	129
	2. Defendants’ Actions Enabled the IRGC’s and Its Proxies’ Terrorist Attacks .....	141
	a. Defendants Helped the IRGC Fund Terrorist Attacks Using Revenue from Large-Scale Cryptocurrency Mining Operations .....	141
	b. Defendants’ Actions Enabled the IRGC to Profit from Ransomware Operations That Funded Terrorist Attacks .....	145
	c. Defendants’ Actions Enabled the IRGC to Efficiently Fund Its and Its Proxies’ Terrorist Attacks .....	146
	B. Hamas’s and PIJ’s Attacks on Plaintiffs .....	149
	C. Al-Qaeda’s Attacks on Plaintiffs .....	156
	D. ISIS’s Attacks on Plaintiffs .....	158
VII.	Defendants’ Unlawful Conduct Had A Substantial Nexus To New York And The United States .....	162
	A. Binance’s Unlawful Conduct Had a Substantial Nexus to New York and the United States Through Binance’s New York Contacts Under Rule 4(k)(1)(A) .....	163
	1. Binance Used New York Customers in Carrying Out the Scheme .....	163
	2. Binance Used New York Partners in Carrying Out the Scheme .....	164

3. Binance Used New York Banks in Carrying Out the Scheme.....	167
B. Alternatively, Binance’s Unlawful Conduct Had A Substantial Nexus To the United States Through Binance’s U.S.-Wide Contacts Under Rule 4(k)(2) .....	168
1. Binance Illegally Operated an Unlicensed Money Transmitting Business Wholly or in Substantial Part in the United States by Serving a Substantial Number of U.S. Users .....	168
2. Binance Used U.S. Banks, U.S. Customers, and U.S. Business Partners in Carrying Out Defendants’ Scheme .....	171
3. Binance Used One or More U.S.-Based Technology Service Provider(s) in Carrying Out Defendants’ Scheme .....	171
C. Zhao’s Unlawful Conduct Had a Substantial Nexus to New York and the United States .....	172
VIII. Plaintiffs Were Killed Or Injured In Terrorist Attacks Committed, Planned, Or Authorized By Foreign Terrorist Organizations That Defendants Supported.....	173
A. The IRGC-Sponsored Attacks by Hezbollah and Kataib Hezbollah in Iraq .....	173
1. The November 7, 2022 Hostage-Taking Attack in Iraq (Troell Family).....	173
2. The December 27, 2019 Rocket Attack in Iraq (Hamid Family) .....	174
3. The January 8, 2020 Attack in Iraq (Al Asad Air Base Attack).....	176
4. The March 11, 2020 Rocket Attack in Iraq (Covarrubias Family).....	219
5. The September 28, 2022 Rocket and Drone Attack in Iraq (Mahmoudzadeh Family).....	221
B. The IRGC-Sponsored Attacks by Hezbollah, Hamas, and PIJ in Israel.....	224
1. The October 7, 2023 Attack in Israel (Brauner and Gabay) .....	224
C. The IRGC’s Hostage Taking Attacks in Iran and the United States.....	226
1. The August 2019 Hostage-Taking Campaign in the United States (Amir Fakhravar) .....	226
2. The September 28, 2019 Hostage-Taking Attack in Iran (Akbar Lakestani) .....	227

D. The IRGC-Sponsored Attacks by Al-Qaeda in Afghanistan and Kenya .....	229
1. The August 7, 2016 Hostage-Taking and Torture in Afghanistan (King Family).....	229
2. The January 14, 2019 Suicide Bombing Attack in Afghanistan (Kamaleson Family).....	230
3. The July 13, 2019 Small Arms Attack in Afghanistan (Sartor Family) .....	232
4. The July 29, 2019 Insider Attack in Afghanistan (Kreischer and Nance Families) .....	233
5. The January 5, 2020 Complex Attack in Kenya (Harrison and Mayfield Families) .....	236
6. The January 31, 2020 Hostage-Taking Attack in Afghanistan (Frerichs Family).....	239
E. The ISIS Attacks in Niger, Syria, and Afghanistan .....	240
1. The October 4, 2017 Complex Attack in Niger (Black, Johnson, and Johnson Families) .....	240
2. The January 16, 2019 Suicide Bombing Attack in Syria (Farmer, Taher, and Wirtz Families).....	243
3. The August 26, 2021 Suicide Bombing Attack in Afghanistan (Gee, Gretzon, and Schmitz Families).....	246
CLAIMS FOR RELIEF .....	250
JURY DEMAND .....	260
PRAYER FOR RELIEF .....	260

## **INTRODUCTION**

1. This civil action arises under the Anti-Terrorism Act, 18 U.S.C. § 2333, as amended by the Justice Against Sponsors of Terrorism Act (“JASTA”), Pub. L. No. 114-222, 130 Stat. 851 (2016), which created a cause of action against those who aid and abet acts of international terrorism that were committed, planned, or authorized by designated foreign terrorist organizations (FTOs).

2. The attacks in this case were committed, planned, or authorized by one or more designated FTOs, including Iran’s Islamic Revolutionary Guard Corps (IRGC), Hezbollah, Hamas, Palestinian Islamic Jihad (PIJ), Kataib Hezbollah, al-Qaeda, and the Islamic State in Iraq and Syria (ISIS). The attacks occurred from 2017 to 2023, and affected 270 direct and indirect victims, who are the Plaintiffs.

3. Since its founding as a global cryptocurrency exchange in July 2017, Binance and its then-Chief Executive Officer Changpeng Zhao aided and abetted these attacks by knowingly facilitating the transfer of millions of dollars’ worth of cryptocurrency to and from terrorist groups. Through this conscious, voluntary, and culpable misconduct, Defendants have enabled FTOs to commit terrorist attacks on Americans, including the attacks that injured Plaintiffs.

4. This action arises against the backdrop of enforcement actions by the U.S. government against Binance and Zhao, which were resolved in November 2023 with guilty pleas and settlements between Defendants and multiple U.S. government agencies including the Department of Justice (DOJ), the United States Department of the Treasury’s Office of Foreign Assets Control (OFAC), the Financial Crimes Enforcement Network (FinCEN), the Commodities Futures Trading Commission (CFTC), and the Internal Revenue Service (IRS).<sup>1</sup>

---

<sup>1</sup> The Securities and Exchange Commission (SEC) has brought a separate action against Binance.

5. Collectively, these government agencies determined that Binance and Zhao willfully violated fundamental legal obligations imposed on all money service businesses and financial institutions. Binance's willful violations included refusing to properly register itself with U.S. authorities, refusing to establish an effective anti-money laundering ("AML") program, refusing to monitor and report suspicious transactions, and violating sanctions—all of which it did deliberately to gain a business advantage. Zhao's violations included willfully aiding and abetting, and causing, Binance to fail to develop, implement, and maintain an effective AML program.

6. As Treasury Secretary Janet Yellen explained, "[a]ny institution, wherever located, that wants to reap the benefits of the U.S. financial system must also play by the rules that keep us all safe from terrorists, foreign adversaries, and crime or face the consequences." Binance, however, "turned a blind eye to its legal obligations in the pursuit of profit. Its willful failures allowed money to flow to terrorists, cybercriminals, and child abusers." The DOJ similarly explained that "Binance's and Zhao's willful violations of anti-money laundering and sanctions laws threatened the U.S. financial system and our national security."

7. To resolve the government's allegations, Binance and Zhao agreed to pay over \$4 billion—one of the largest corporate penalties in U.S. history. Binance also agreed to ongoing monitoring and substantial reform of its practices. Zhao was sentenced to prison time, and agreed to step down as CEO of Binance. Binance and Zhao also admitted many of the facts that give rise to this action.

8. The penalties Binance and Zhao have paid constitute partial remuneration to the financial system and the government. But they are far from adequate. Binance and Zhao are worth tens of billions of dollars, which they made by willfully prioritizing the growth of their

business over compliance with the law and basic decency. More specifically, they earned this wealth by courting dangerous customers, knowingly facilitating terrorist financing or willfully blinding themselves to that fact. Terrorist attacks on Americans—including the specific attacks at issue in this case—were an obviously foreseeable risk of the assistance Binance and Zhao willfully rendered to terrorist actors. Binance and Zhao thus enabled terrorist violence, and should be held accountable not only to governments and regulators, but also to the flesh-and-blood victims of the attacks they aided.

9. It is the “long-standing policy of the United States that civil lawsuits against those who support, aid and abet, and provide material support for international terrorism serve the national security interests of the United States by deterring the sponsorship of terrorism and by advancing interests of justice, transparency, and accountability.” Sudan Claims Resolution Act, Pub. L. No. 116-260, div. FF, tit. XVII, § 1706(a)(1), 134 Stat. 3294 (2020). To advance that policy objective, Congress explained that JASTA seeks “to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief against persons, entities, and foreign countries, wherever acting and wherever they may be found, that have provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities against the United States.” JASTA § 2(b).

### **THE PARTIES**

10. Plaintiffs are 102 direct victims and 168 indirect victims of terrorist attacks committed from 2017 to 2023. In this terminology, direct attack victims are those who were physically injured or killed in the attack. Indirect attack victims are the direct attack victims’ close family members who suffered financially and emotionally as a result of the attacks. They

include spouses, children, parents, siblings, and other close relations of the direct attack victims.

Each Plaintiff is either a U.S. national or the estate, survivor, or heir of a U.S. national.<sup>2</sup>

11. Defendant **Binance Holdings Limited** d/b/a Binance and Binance.com (“Binance”) is an entity incorporated in the Cayman Islands that held, among other things, intellectual property, including trademarks and domain names, employment contracts for certain employees operating Binance.com, and has employed at least certain individuals who perform work on behalf of the Binance platform. Since at least July 2017, Binance has operated a web-based virtual currency exchange under the name Binance.com. That exchange offered and still offers trading in virtual currencies, digital asset commodities and related derivatives, among other financial products and services, to over 100 million customers throughout the world, in volumes equivalent to trillions of U.S. dollars.

12. On November 21, 2023, Binance pleaded guilty to federal charges of failing to maintain an effective anti-money laundering program and entered into settlements with three U.S. regulators in connection with charges of violations of the Bank Secrecy Act and U.S. sanctions. These violations included knowingly processing and refusing to report transactions involving cryptocurrency wallets held by or affiliated with terrorist groups.

13. Defendant **Changpeng Zhao** is the primary founder, majority owner, and former CEO of Binance. Zhao launched Binance in 2017 and from that time until he was removed from

---

<sup>2</sup> The term “estate” as used herein encompasses established estates, anticipated estates, as well as certain estate-like constructs available under the laws of certain States (such as “heirships”). The process of establishing certain estates is ongoing, and the identified family members or other individuals, as the anticipated personal representatives, bring these claims on behalf of the anticipated estates of such decedents and all heirs thereof. Each person so identified reserves all rights, including the right pursuant to Fed. R. Civ. P. 25, to seek to substitute for itself the decedent’s estate, any successor thereto, or any subsequently named and/or designated estate representative.

the role as part of his criminal guilty plea with the DOJ, he had ultimate control over all of Binance's business activities. Zhao is a dual citizen of Canada and the United Arab Emirates who is currently serving a four-month long prison sentence in California in connection with his criminal guilty plea.<sup>3</sup> Zhao has directly or indirectly owned the scores of entities that collectively operate the Binance platform.

14. Together with a core senior management group, as Binance's CEO, Zhao made strategic decisions for Binance and supervised and exercised day-to-day control over its operations and finances. Zhao was responsible for all major strategic decisions, business development, and management of the Binance enterprise. Zhao was responsible for directing and overseeing the creation and operation of Binance's trade matching engines, website, application programming interface ("API") functionalities, and order entry system. And Zhao was ultimately responsible for evaluating the legal and regulatory risks associated with Binance's business activities. Zhao has admitted that at all relevant times he "prioritized Binance's growth and profits over compliance with U.S. law, telling Binance employees that it was 'better to ask for forgiveness than permission.'"

15. On November 21, 2023, Zhao pled guilty to willful violations of the Bank Secrecy Act. He agreed to personally pay a \$150 million fine and was sentenced to four months in prison on April 30, 2024. Zhao was also a named party with "control person" liability in regulatory settlements with Binance.

16. Zhao and Binance have admitted that "Zhao made the strategic decisions for" the entire Binance enterprise and "exercised day-to-day control over its operations and finances,"

---

<sup>3</sup> Zhao is scheduled to be released from federal custody on September 29, 2024.

while being “publicly dismissive of ‘traditional mentalities’ about corporate formalities and their attendant regulatory requirements.”

17. Zhao has publicly acknowledged that he and the broader Binance enterprise are alter egos of one another, claiming that “Wherever I sit is the Binance office. Wherever I meet somebody is going to be the Binance office.” According to Zhao, the concept of a formal corporate entity with a headquarters and its own bank account is unnecessary: “All of those things doesn’t have to exist for blockchain companies.”

18. The District Court for the Northern District of Illinois has found as fact that Defendant Zhao “directly or indirectly owned and controlled dozens of corporate entities incorporated in numerous jurisdictions around the world” that collectively “operate the Binance platform as a common enterprise.”

19. The court further determined that “Binance’s reliance on [this] maze of corporate entities to operate the Binance platform is deliberate; it is designed to obscure the ownership, control, and location of the Binance platform.”

20. True to their dismissive attitude about corporate formalities, Zhao and Binance freely commingled funds with each other and multiple Binance subsidiaries and affiliates and non-Binance entities ultimately controlled by Zhao; exercised direct control over operations and decisions of purportedly independent entities; dealt with affiliates and subsidiaries on a non-arm’s-length basis; and maintained signatory authority and control over such entities’ bank accounts.

21. Zhao and Binance abused the corporate form to perpetrate frauds on U.S. regulators and the public, and to perpetuate their scheme for providing financial services to international terrorists and criminals.

22. For example, when Zhao and Binance established a U.S. platform—Binance.US, operated by Zhao-controlled BAM Trading Services—that they portrayed as ‘regulatory compliant’ to divert regulatory attention away from Binance itself, Zhao and Binance were secretly “integrally involved in the operation” of that platform. Their role included not only “control[ing] BAM Trading’s routine business expenditures and decisions,” but also retaining authority and control over BAM Trading’s bank accounts and commingling its funds with Binance funds in accounts at another entity controlled by Zhao. Zhao and Binance retained signatory authority over BAM Trading’s accounts (and thus Binance.US customers’ funds) until at least May 2023.

23. According to the SEC, “[g]iven its control over BAM Trading’s bank accounts, Binance’s finance team was also able to make substantial fund transfers without BAM Trading’s knowledge.” Zhao and Binance’s surreptitious control over BAM Trading and Binance.US—which they repeatedly and publicly denied—eventually led BAM Trading’s CEO to resign, explaining his realization that “CZ [*i.e.*, Zhao] was the CEO of BAM Trading, not me.”

24. Zhao and Binance persistently dealt with BAM Trading on a non-arm’s-length basis. In addition to controlling its operations and bank accounts, they allowed BAM Trading to use proprietary Binance software for at least six months without executing any formal licensing agreements.

25. On information and belief, Zhao and Binance dominated the deliberately labyrinthine “maze” of other Binance subsidiaries and affiliates in the same manner that they dominated BAM Trading.

26. Because of Zhao’s domination of Binance, and Zhao and Binance’s domination of the other entities within the corporate “maze” of the Binance enterprise, actions purportedly performed by those entities are legally attributable to Zhao and Binance.

### **JURISDICTION AND VENUE**

27. This Court has subject-matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2333(a), which provides for jurisdiction over civil actions brought by citizens of the United States, their estates, and family members who have been killed or injured by reason of acts of international terrorism.

28. Personal jurisdiction exists over Binance under Federal Rule of Civil Procedure 4(k)(1)(A) and New York Civil Practice Law and Rules § 302(a)(1) based on Binance’s use of New York banks, customers, and business partners in carrying out Defendants’ scheme.

29. Alternatively, personal jurisdiction exists over Binance under Federal Rule of Civil Procedure 4(k)(2), based on Binance’s illegal operation of an unlicensed money transmitting business wholly or in substantial part in United States by serving a substantial number of U.S. users in the United States through Binance’s cryptocurrency exchange in the United States. Rule 4(k)(2) jurisdiction also exists over Binance based on Binance’s use of New York banks, New York customers, New York business partners, and U.S.-based Amazon in carrying out Defendants’ scheme. Rule 4(k)(2) jurisdiction also exists over Binance because Binance purposefully targeted the United States through Binance’s participation in Defendants’ scheme to connect terrorist users outside the United States with counterparties inside the United States to maximize Binance’s profits through the unrivaled size of the U.S. marketplace while Binance simultaneously schemed to facilitate, and profit from, FTOs’ ransom payments from U.S. victims of acts of international terrorism, including U.S.-origin ransoms paid to FTOs to secure the release of hostages and/or the recovery of data stolen during a ransomware attack,

which caused tortious effects on and within the United States. Simply put, Binance participated in such attacks within the United States. If the Court were to find jurisdiction over Binance lacking under New York's long-arm statute, Plaintiffs certify based on the reasonably available information that Binance would not then be subject to suit in the courts of general jurisdiction of any other state, which would make Rule 4(k)(2) jurisdiction appropriate.

30. Personal jurisdiction exists over Zhao under Federal Rule of Civil Procedure 4(k)(1)(A) and New York Civil Practice Law and Rules § 302(a)(1) as an individual corporate officer who supervised and controlled the activity subjecting Binance to jurisdiction above. Rule 4(k)(1)(A) jurisdiction also exists over Zhao because he conspired with Binance and other agents to conceal their illegal operation of an unlicensed money transmitting business and agents acting at Zhao's direction engaged in overt acts in New York on Zhao and Binance's behalf, including aiding New York-based trading firms in circumventing technological controls to supply needed liquidity to Binance's platform. Rule 4(k)(1)(A) jurisdiction also exists over Zhao because he owned and controlled multiple offshore entities that maintained accounts at Signature Bank in New York and were the counterparties to many large transactions with Binance totaling in the hundreds of millions of dollars from at least 2019 through at least 2023. Alternatively, personal jurisdiction exists over Zhao under Federal Rule of Civil Procedure 4(k)(2) as an individual corporate officer who supervised and controlled the U.S. activity subjecting Binance to jurisdiction, as set forth above. Rule 4(k)(2) jurisdiction also exists over Zhao because he purposefully targeted the United States through Zhao's participation in Defendants' scheme to connect terrorist users outside the United States with counterparties inside the United States to maximize Binance's profits through the unrivaled size of the U.S. marketplace while he simultaneously schemed to facilitate, and profit from, FTOs' ransom payments from U.S. victims

of acts of international terrorism, including U.S.-origin ransoms paid to FTOs to secure the release of hostages and/or the recovery of data stolen during a ransomware attack, which caused tortious effects on and within the United States. Simply put, Zhao participated in such attacks within the United States. If the Court were to find jurisdiction over Zhao lacking under New York’s long-arm statute, Plaintiffs certify based on the reasonably available information that Zhao would not then be subject to suit in the courts of general jurisdiction of any other state, which would make Rule 4(k)(2) jurisdiction appropriate.

31. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b)(2), based on Defendants’ use of at least one bank in this District in carrying out their scheme. Alternatively, venue is proper in this District under 28 U.S.C. § 1391(c)(3) and/or § 1391(d).

### **CRYPTOCURRENCY PRIMER**

32. Cryptocurrencies are digital assets designed to serve as a medium of exchange or store of value. They differ from traditional “fiat” currencies because they are not issued by a central institution or backed by the full faith and credit of a government. And despite the individual units of a particular cryptocurrency being referred to as “coins” or “tokens,” there is no physically tangible version of such units—whereas a significant amount of fiat currency is invariably printed and minted and thus available to spend and transact in the form of paper bills and metal coins. Each individual cryptocurrency unit has its own unique identifier, which is one of the features that helps secure them.

33. Cryptocurrencies are typically secured by users in “crypto wallets.” A crypto wallet is not an actual wallet per se but a software program that that allows “owners” of cryptocurrencies to store and manage the information necessary to identify and transfer their digital assets. Each crypto wallet has its own address, also referred to as a “public key,” which is expressed as a long string of numbers and letters. This address can be shared with others, who

can use this information to transfer to, or transact with, the owner of that crypto wallet. Each crypto wallet has a similarly complex “private key,” which functions as that wallet owner’s secure passcode. That passcode is necessary to access cryptocurrency from one’s crypto wallet and transfer it to another crypto wallet.

34. Cryptocurrencies are secured and transferred between crypto wallets using distributed ledger technology, which is often referred to as a “blockchain.” A blockchain is a database spread across multiple computer servers that vets or verifies every cryptocurrency transaction between crypto wallet addresses using a specified mathematical process. Once verified, each cryptocurrency transaction is recorded permanently on the blockchain and viewable by any individual. Many cryptocurrencies have their own blockchains, and several blockchains can accommodate a variety of cryptocurrencies.

35. In exchange for the work performed by blockchain participants to validate and record transactions (by adding “blocks” to the blockchain), blockchain protocols provide set rewards, which are often paid in the form of new tokens issued to the designated wallet addresses of those doing the work. Those compensatory tokens are often funded by fees charged by parties transacting on that blockchain and/or the blockchain’s creation of additional tokens of its “native” cryptocurrency.

36. Presently, there are thousands of cryptocurrencies and associated blockchain protocols, each with its own particular use case(s) and suite of benefits that it purports to offer its adopters. The three most popular and widely used cryptocurrencies are Bitcoin, Ether, and Tether. Bitcoin (BTC) is considered the “original” and most well-known cryptocurrency. In the relatively short history of cryptocurrencies, Bitcoin has been the most widely used to purchase real-world and digital goods and services, and as a store of value. Ether (ETH) is the native token

of the Ethereum blockchain and although often used in a manner similar to BTC (*i.e.*, to make payments or as a store of value), it was designed for use in running “smart contracts,” which are programs that automate certain actions between parties to a transaction.<sup>4</sup> Tether (USDT) is the most widely used of a class of cryptocurrencies known as “stablecoins.” Unlike BTC and ETH—which have been known to fluctuate widely in value—the defining feature of Tether is its 1:1 peg to the value of the U.S. Dollar, which it purports to accomplish by backing the currency with a wealth of real-world assets (like U.S. Treasury bills and positions in gold) and select crypto assets (predominantly BTC). Unlike actual U.S. Dollars, however, Tether can be transferred almost instantly across borders without having to “clear” through or otherwise touch the U.S. financial system.

37. Cryptocurrency exchanges like Binance and Coinbase are vital actors in the cryptocurrency ecosystem. Exchanges typically offer brokerage, trading, settlement, and storage services, which collectively allow their customers to purchase and sell a variety of cryptocurrencies using other cryptocurrencies or fiat currency without having to locate and deal with specific crypto wallet address(es) to stand on the other side(s) of that transaction. Importantly, exchanges operate as centralized depositories for digital assets that customers deposit or trade on their platforms. The exchanges typically have their own crypto wallets that collectively store the exchange’s own assets plus those of its various customers, which assets are

---

<sup>4</sup> A simple example of such a “smart contract” is as follows: when one person contracts with another to purchase one BTC for 25 ETH tokens, a smart contract could automatically transfer 25 ETH tokens from one designated crypto wallet to another once it receives the promised BTC (in lieu of, for example, transferring the 25 ETH upfront before the BTC is transferred, sending the owner of the wallet that received the BTC a “bill” for 25 ETH after the BTC is transferred, or using a third party payment escrow service to eliminate the same counterparty performance risk).

collectively used to create liquidity pools to facilitate fast and cost-efficient transactions for customers.

38. Customers' assets that are deposited with centralized exchanges like Binance are not typically held in unique crypto wallets belonging to each customer. Rather, each customer has an entitlement to the specific amounts and types of crypto assets it has deposited with the exchange, which is tracked and maintained on the platform's internal ledgers. Whereas transactions between crypto wallets outside of a centralized exchange's platform are all recorded on a publicly available blockchain, transactions taking place on a centralized exchange platform are referred to as "off-chain" and are not recorded the same way. Although this feature of transactions on exchange platforms reduces the public's visibility into the universe of crypto transactions, it is also what makes transactions on such a platform far more cost-efficient for most individual customers (because the exchange can aggregate customer transactions in large blocks before transacting "on-chain" rather than paying fees required by blockchain protocols to validate and record each individual customer's every transaction).

## **FACTUAL ALLEGATIONS**

### **I. From 2003 Through 2024, The Islamic Revolutionary Guard Corps Led A Jihadist “Axis of Resistance” Comprised Of Designated Foreign Terrorist Organizations That Partnered To Conduct Terrorist Attacks Targeting The United States**

39. The IRGC, also known as the “Sepah,” “Pasdaran,” and “Guardians of the Islamic Revolution,” has operated as a global terrorist organization since 1979. Throughout, the IRGC was always a global terrorist organization totally committed to the violent jihadist ideology of Ayatollah Ruhollah Khomeini and Ayatollah Ali Khamenei and tasked with exporting the Islamic Revolution throughout the world through the propagation of terrorist attacks targeting the Ayatollah’s and IRGC’s chief enemy for more than forty years: the United States government.

40. Since 1979, the IRGC has led an alliance of anti-American terrorist organizations, many of which it has supported for decades, and all of which were united by their shared mission of conducting terrorist attacks targeting the United States—directly, by targeting Americans, or indirectly, by targeting United States allies—to coerce U.S. government decisionmakers in Washington, D.C. and elsewhere in the United States to choose to withdraw from the Middle East. That effort has always been directly assisted by the Supreme Leader’s Office (or “SLO”), which Ayatollah Khamenei greatly expanded in 1989-1990 to optimize the Iranian regime’s provision of money, arms, training, and logistical support to IRGC proxies to enable the latter to attack the United States.

41. Since 2003, the IRGC’s and SLO’s terrorist alliance has proudly called itself the “Axis of Resistance” while regularly attacking the United States. In 2019, the Defense Intelligence Agency (“DIA”) reported to Congress:

Throughout its 40-year history, the Islamic Republic of Iran has remained implacably opposed to the United States [and] our presence in the Middle East ... Tehran has committed itself to becoming the dominant power in the turbulent and

strategic Middle East. ... It leads a cohesive if informal bloc of Shia and Alawi state and nonstate actors—its ‘Axis of Resistance’ against the West.

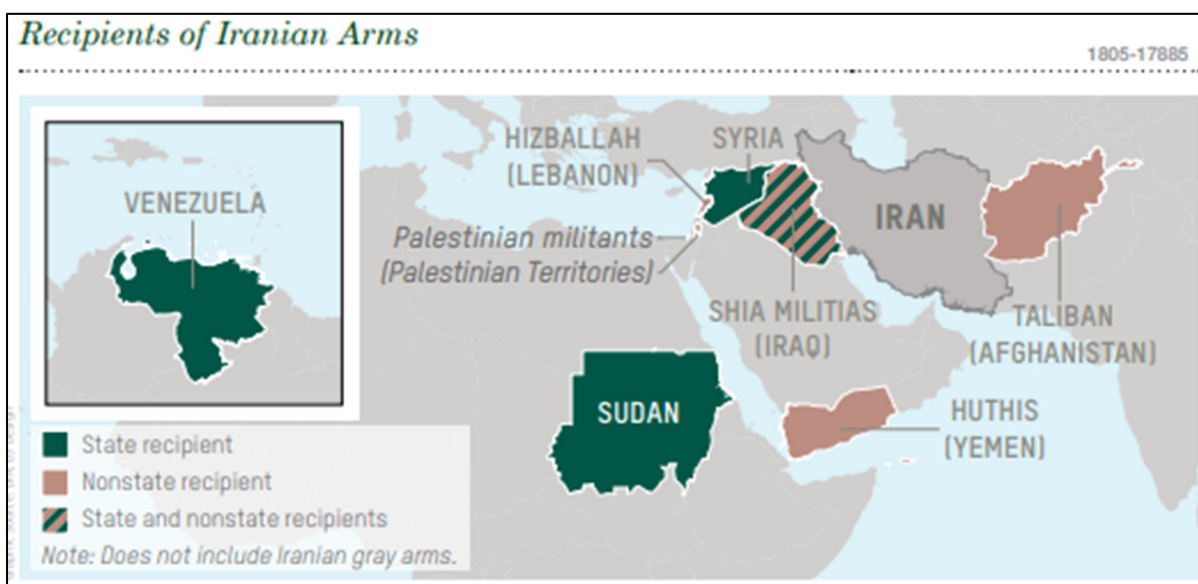
42. The IRGC’s and SLO’s global terrorist alliance functioned as a jihadist analogue to NATO and similar western alliances. It included, among others: (1) Lebanese terrorist group **Hezbollah**, a global terrorist organization that has been an FTO since 1997, which was founded by the IRGC in 1982 and has been its most reliable and notorious proxy ever since; (2) Iraqi terrorist group **Jaysh al-Mahdi** (or “JAM”), which was founded by Hezbollah, publicly identified as Hezbollah’s “striking arm in Iraq,” operated in Baghdad through a joint Hezbollah-JAM cell, and led by Muqtada al-Sadr, including notorious JAM cells known as Jaysh al-Mahdi Special Groups, the most infamous of which were Jaysh al-Mahdi Special Group **Kataib Hezbollah**, and Jaysh al-Mahdi Special Group **Asa’ib Ahl al-Haq**, FTOs since 2009 and 2020, respectively; (3) Palestinian terrorist groups, including **Hamas** (Harakat al-Muqawama al-Islamiya) and **Palestinian Islamic Jihad** (“PIJ”), which have been FTOs since 1997; and (4) **al-Qaeda**.

43. Ayatollah Khamenei was a direct—and key—financial sponsor of each Axis of Resistance member. As he publicly stated in 2015, “we will never stop supporting our friends in the region and the people of Palestine, Yemen, Syria, Iraq, Bahrain, and Lebanon.” “Basically,” Congressman Duncan observed on May 12, 2016, Khamenei meant IRGC proxies like “Hezbollah [and] Hamas.”

44. The Axis of Resistance was not merely a slogan: it had nearly every jihadist function that would parallel a western alliance, including joint attacks—which the terrorists, U.S., U.N., and E.U. all called “operations”—that were committed through the work of joint cells in which two or more FTOs were co-located with one another for a common anti-American purpose, supported by joint training, procurement, financial support, logistics, basing, and

intelligence. In Iran, for example, the regime maintained multiple complexes in which the IRGC, Qods Force, Hezbollah, Hamas, PIJ, and JAM trained, studied, and plotted together as one coordinated syndicate of terrorists who worked together to target the United States and sought to coerce the U.S. government to withdraw from the Middle East.

45. According to a graphic published by the DIA in a 2019 report to Congress, Hezbollah, Hamas, PIJ, and JAM were part of the “Axis of Resistance,” as shown by the DIA’s map of IRGC arms shipments intended to sponsor attacks to drive the United States out of the Middle East, inclusive of Muslim-majority parts of Africa and Southwest Asia:



46. Notably, the name “Axis of Resistance” itself targeted the United States because its members “resist” the U.S. presence in the Middle East.<sup>5</sup> Part of this “resistance” included

<sup>5</sup> “Resistance” refers to terrorist attacks targeting the United States (including through its allies like Israel and Iraq) under the IRGC’s constitutional mandate to export Iran’s Islamic Revolution. “Resistance” is the preferred euphemism of the IRGC and every IRGC proxy, many of which, including Hezbollah and Hamas, literally feature the word “Resistance” in the Arabic version of their “external operations wing” (in the case of Hezbollah) and name itself (in the case of Hamas). “Resistance Movements”—including its alternative variants, “Jihad Movements” and “Liberation Movements”—refers to the IRGC’s terrorist proxy members in its “Axis of Resistance.”

sponsoring waves of terrorist attacks against Israelis. But even that targeted the United States because the terrorists believed Israel to be an agent of America and believed that the United States was key to whether they could overthrow the Israeli government and replace it with their shared goal of an Islamic caliphate that governed Jerusalem, which they called “Qods.”

47. Other than the Plaintiffs attacked by ISIS, *infra* at Part VIII(E), each Plaintiff was injured in IRGC-sponsored attacks in Iraq, Iran, Israel, Afghanistan, Kenya, and/or the United States from 2018 through 2023 that were committed by one or more of the IRGC, including the IRGC Qods Force and the IRGC Intelligence Organization, Lebanese Hezbollah, JAM (inclusive of Kataib Hezbollah), Hamas, PIJ, and/or al-Qaeda. For some instances, the IRGC sponsored the attack by funding the proxy and/or proxies that committed the attack (*e.g.*, funding Hamas prior to October 7) or by providing or funding arms that supported the attack, while attacks were committed, planned, or authorized by Hezbollah, Hamas, PIJ, and/or JAM. Some attacks were committed jointly by Hezbollah and/or Hamas and/or PIJ (in Israel), or by Hezbollah and Kataib Hezbollah (in Iraq).

#### **A. The Islamic Revolutionary Guards Corps**

##### **1. The IRGC Was an Integrated Global Terrorist Organization**

48. The IRGC was an integrated terrorist organization. From 2011 through 2024, the IRGC had eight branches, all of which were ultimately accountable to Ayatollah Khamenei, and all of which but the Qods Force also reported IRGC Commander-in-Chief Mohammad Ali Jafari (from 2011 through 2019) and Hossein Salami (from 2019 through present) and their respective deputies (Salami as Jafari’s deputy from 2011 through 2019), and Ali Fadavi as Salami’s deputy from 2019 through present.

49. *First*, the IRGC Qods Force (“Qods Force” or “IRGC-QF”) was always the IRGC’s primary external operations arm and had lead responsibility for the IRGC’s terrorist

attacks outside Iran. Qassem Soleimani led the IRGC-QF from 2011 through his death on January 2, 2020, after which Ayatollah Khamenei handed leadership to Esmail Ghaani, who led the IRGC-QF from 2020 through present.

50. *Second*, the IRGC Intelligence Organization (or “IRGC-IO”) was always the Iranian regime’s largest, most powerful, and most lethal intelligence arm and played a key role alongside the Qods Force (for whom it embedded in operations outside of Iran) in IRGC attacks outside Iran, and had lead responsibility for attacks committed, in part, inside Iran, *e.g.*, hostage taking of dual nationals. Hossein Taeb led the IRGC-IO from 2009 through June 23, 2022, when he was transferred to serve as a senior advisor to the SLO and was replaced by Mohammad Kazemi, who has always led it since.

51. *Third*, the IRGC Aerospace Force (or “IRGC-ASF”) was the IRGC’s arm jointly responsible (alongside the IRGC-QF and IRGC-IO) for executing IRGC-supported missile and unmanned aerial vehicle (“UAV”) attacks, as well as other air attack functions. The IRGC-AF included the IRGC-Aerospace Force Al-Ghadir Missile Command (or “IRGC-ASF-AGMC”), which shared responsibility for missile attacks alongside the IRGC-QF and IRGC-IO. From 2009 through present, Amir Ali Hajizadeh commanded the IRGC-ASF, Mahmud Bagheri commanded the IRGC-ASF-AGMC, and Mohammad Agha Ja’fari served as a senior IRGC-ASF-AGMC who helped lead it alongside Bagheri—who were tasked with optimizing every facet of the IRGC’s development of, logistics for, and transfer of, IRGC missiles to IRGC branches and IRGC proxies, including Hezbollah and Hamas.

52. *Fourth*, the IRGC Basij, meaning “mobilization” (“Basij” or “IRGC-B”) was the IRGC’s chief recruitment, propaganda, morality police, and mass mobilization arm, and was commanded by Gholamreza Soleimani.

53. *Fifth*, the IRGC Ground Resistance Force (or “IRGC-GRF”) was the IRGC’s border and internal armored organization, and was commanded by Mohammad Pakpour.

54. *Sixth*, the IRGC Navy (or “IRGC-N”) was the IRGC’s naval organization that smuggled terrorists, weapons, and funds, and harassed of U.S. military vessels, in the Persian Gulf, and was commanded by Alireza Tangsiri.

55. *Seventh*, the IRGC Counterintelligence Organization (or “IRGC-CIO”) was the IRGC’s counterintelligence arm tasked with preventing the U.S. intelligence community, including but not limited to the CIA and DIA, from acquiring actionable intelligence that could prevent IRGC-sponsored attacks targeting the United States, and was commanded by Mohammad Kazemi.

56. *Eighth*, the IRGC Intelligence Protection Organization (or “IRGC-IPO”), which was sometimes also called the IRGC Security Force, was the IRGC’s arm responsible for securing key locations of interest for the IRGC, *e.g.*, airports secured by the IRGC-IPO so that operatives from the IRGC-IO can maximize the ability of the IRGC to use an airport as a location to conduct hostage-taking attacks and gather intelligence in support of the same, and was led by Fathollah Jomeiri.

## **2. The IRGC Was Purpose-Built to Attack the United States as Its Primary Mission**

57. The IRGC always targeted the United States for terrorist violence. Iran’s 1979 revolution was militantly anti-American, and Iran’s regime continued such approach ever since. Since 1979, the IRGC regularly engaged in and supported acts of terrorism directed at the United States, which targeted the U.S. government in Washington, D.C. by seeking to coerce it into changing U.S. policy as sought by the IRGC, including the United States’s exit from the Middle East and abandonment of its allies there, including Israel.

58. Indeed, unlike most terrorist groups, the IRGC was specifically established to target the United States as its primary enemy. The IRGC's doctrinal and institutional targeting of the United States was a product of Iran's history with America, and the IRGC founders' understanding that the United States posed a direct threat to the viability of their nascent terrorist enterprise. In 2011, for example, the U.S. Department of Defense (DoD) published a declassified analysis about the IRGC and its proxies that warned: "The terrorism pillar of [IRGC Commander] Jafari's strategy relies on intimidating potential adversaries and their supporters through the threat of terrorist activities against non-military targets in their territories ... [through] an attack [committed by IRGC proxy] ... [t]errorist organizations like ... Lebanese Hezbollah [and] Khattab Hezbollah in Iraq, ... [which] act[ed] on behalf of Iran's [*i.e.*, the IRGC's] interests." As Qasem Soleimani publicly enthused in his posthumous autobiography, "All of you loved Imam [*i.e.*, Ayatollah Khomeini] and believed in his path. [Ayatollah Khomeini's] path was the path of fighting against the U.S. and supporting the Islamic Republic and the Muslims, who are [O]ppressed by the Arrogant Powers [*i.e.*, the United States government and its allies, including Israel], under the flag of *Wilayat-e-Faqih* [*i.e.*, Ayatollah Khomeini's system of rule of the jurisprudent]."

59. Ayatollah Khomeini established the IRGC to target the United States, in line with his own view that the U.S. government posed the greatest threat to the IRGC's transnational terrorist agenda. Representative examples of Ayatollah Khomeini's pronouncements to that effect included, but were not limited to, as follows:

- a. "America is the archenemy of the Oppressed people of the world."
- b. "Today, America is the number one enemy."
- c. "Let brotherly Arab nations and the Palestinian and Lebanese brothers know that all their miseries are caused by America."

- d. “The criminal hands of the world arrogant states [*i.e.*, the United States and its “puppets”] will not be severed off the Islamic lands unless the Muslim nations and the oppressed people rise up against them [*i.e.*, the United States] and their offspring especially Israel.”
- e. “Cold and warm weapons, that is, pens, words and machineguns should all be aimed at the enemies of mankind, headed by America.”
- f. “We believe that the Muslims should unite and together slap America, and know that they can do it!”
- g. “O the Oppressed people of the world! From whatever country you come and from whatever stratum you come, arise and do not fear the yelling and ruckus of America and other powers, and make the world too narrow and tight for them.”
- h. “Confronting America is presently above all our problems. If today our forces become divided, it benefits America. Right now, America is the enemy and all our equipment should be aimed at this enemy.”

60. Under Iran’s constitution, as interpreted by the Ayatollah and the IRGC, the IRGC interprets its sole responsibility for protecting and exporting the Islamic Revolution as the IRGC’s specific responsibility to sponsor terrorist attacks targeting the United States, which the IRGC always understood to be the top threat to the Islamic Revolution. For the IRGC, exporting the revolution meant one thing: IRGC-sponsored terrorist attacks, usually committed by notorious IRGC proxies, targeting the United States in the Middle East.

61. Ayatollah Khomeini was the IRGC’s founder and leader, but was never an IRGC “member” who was himself responsible for IRGC-sponsored attacks. In contrast, Ayatollah Khamenei was always a sworn brother of the IRGC, with the rank of Brigadier General, who led IRGC forces during the Iran-Iraq war, before he became leader of the Islamic Revolution and overall commander of the IRGC as the Supreme Leader. As a lifelong IRGC member and supporter, Khamenei, among other things, previously served as Supervisor of the IRGC, as Ayatollah Khomeini’s Representative in the High Security Council, and as an active IRGC commander at the frontlines of the Iran-Iraq War.

62. At all times, Khamenei was a prominent, and important, direct sponsor of acts of terrorism in his capacity as leader of the IRGC. To that end, Khamenei appointed representatives who served in key IRGC divisions and the IRGC's leadership.

63. Unsurprisingly given his IRGC pedigree, Khamenei was widely known as a staunch supporter of terrorism. On June 29, 2009, for example, *Newsweek* reported:

Since his early days immersed in scripture and poetry, [Khamenei] had loved to identify with “the [O]ppressed,” and he built his base of support in those institutions—the clergy, the military and the bureaucracy .... Since the war years in the 1980s, he had also forged close relations with the intelligence apparatus, perhaps convincing himself, as many a revolutionary has done, that the best way to prevent oppression is to eliminate enemies. In an article published [in 2008] in *Foreign Affairs*, Iranian dissident Akbar Ganji claimed that at Khamenei's very first meeting with cabinet leaders after taking his post as Supreme Leader in 1989, he put forth a ‘theory of terror’ that would define his approach to security issues. “The majority of the people in the state are silent,” he is supposed to have said. But “a selfless group of individuals can make the state endure by using terror.”

64. Khamenei, like Khomeini, emphasized that “Resistance”—code for IRGC-sponsored acts of terrorism targeting the United States—was the foundation of the IRGC's mission and associated ideology. At a widely covered June 4, 2007 event honoring Khomeini, for example, Khamenei emphasized that, although “Resistance against bullying powers in order to attain one's rights has a price ... You should not beg others for your rights. As long as you retreat and show leniency, the hegemonic nature of the bullying powers will increase their intimidation. Rights must be achieved through resistance.”

65. Khamenei was a key, direct sponsor of Hezbollah, Hamas, and PIJ attacks in Israel—and proud of it. On February 27, 2010, for example, *Agence France Presse's* reporting about Hamas noted that “Iranian supreme leader Ayatollah Ali Khamenei told Palestinian militant chiefs that sustained resistance was the key to liberating their land.” On August 4, 2014, similarly, IRGC arm *Fars News Agency* reported: “A few days ago and following first-time

remarks by Supreme Leader of the Islamic Revolution Ayatollah Seyed Ali Khamenei, a large number of ... IRGC Commanders underlined the necessity for all Islamic countries to supply weapons and military tools and equipment to the Palestinians to help them defend themselves against the Israeli attacks.” As Jeffrey Goldberg of *The Atlantic* observed on March 9, 2015:

[A]s a reminder to those who argue that Jews should stop worrying so much about people who threaten to kill them, here is some (just some) of what [Ayatollah Ali Khamenei] ... ha[s] said about Israel: ...

- “It is the mission of the Islamic Republic of Iran to erase Israel from the map of the region.” (2001) ...
- “The Zionist regime is a cancerous tumor and it will be removed.” (2012) ...
- “This barbaric, wolf like & infanticidal regime of Israel which spares no crime has no cure but to be annihilated.” (2014) ....

66. IRGC members directly swore allegiance to the Ayatollah, not to the Iranian regime, and were therefore, as Iran scholar Seth Frantzman publicly observed in 2021, “solely controlled and commanded by Vali-e-Faqih,” *i.e.*, the Ayatollah’s exclusive rule, which “ma[de the] IRGC ... strongly akin to ISIS.”

67. As the United States has confirmed, the IRGC was always a terrorist organization that serially violated the laws of war through the terrorist attacks it sponsored. On April 8, 2019, Secretary of State Pompeo observed: “[t]he IRGC masquerades as a legitimate military organization, but none of us should be fooled. It regularly violates the laws of armed conflict; it plans, organizes, and executes terror campaigns all around the world.”

68. The IRGC—inclusive of each IRGC component—always practiced terrorism as a matter of doctrine. On October 12, 2011, for example, DoD published an analysis of the IRGC that confirmed as follows:

In ... 2005, when he was the commander of the IRGC Center for Strategy, [Mohammad Ali] Jafari stated, ‘As the enemy [*i.e.*, the United States] is far more

advanced technologically than we are, we have been using what is called asymmetric warfare methods [*i.e.*, acts of terrorism targeting the United States]... The tenets of this doctrine include, but are not limited to ...: incorporation of ... terrorism .... In May 2004, Hassan Abbasi, the Director of the Center for Doctrinal Studies at the IRGC's Imam Hussain University bluntly summarized the IRGC's intent to employ terrorist tactics, "The Islamic world needs suicide bombers... I am a theoretician of terror and violence... We are proud of terrorism, which makes the foundations of unbelief tremble... We have identified the US' Achilles heel and have coordinated with terrorist organizations... We caused the US economic growth to drop and we will cause its disintegration."

69. Nobody ever actually "retires" from the IRGC. Instead, IRGC officials who "retire" are typically simply moved from uniform-wearing positions into ostensibly civilian-facing roles that serve as fronts for key IRGC operations, including fundraising and logistics. For example, according to an analysis of the IRGC published by NATO in 2020: "The IRGC acts as a business fraternity within which members of the Guard can progress along a prescribed career path. Following active service, IRGC members are offered senior positions in state-affiliated [] organisations and [] networks ... Accordingly, 'no one ever leaves the IRGC'; its senior officers are viewed as an Iranian 'freemasonry' and 'Ivy League network', signalling that the IRGC exceeds ideological devotion."

70. The IRGC exercised programmatic control over the profits and technologies generated by its fronts, black market activities, mandatory 10%-20% *khums* donation required of all IRGC members on all transactions, and taxation schemes to maximize the IRGC's ability to convert such value into acts of terrorism targeting the United States. As *Radio Free Europe* reported on September 18, 2009, "all the IRGC's economic activities are monitored only by internal IRGC auditors." Among other ways, the IRGC accomplished this through the Logistics Policy Directive that governed since 2003, which mandated that IRGC profits be spent on its operations. *See infra* ¶ 393.

71. At all relevant times, the IRGC provided key weapons-related support to its proxies, which directly enhanced the ability of the IRGC and its proxies to target and kill Americans throughout the world. The IRGC's aid to JAM in Iraq was typical of how it aided other close proxies, including Hamas. As DoD reported to Congress in April 2010:

[T]he IRGCQF posts its officers in Iran's diplomatic missions throughout Iraq, including Iran's ... Ambassador to Iraq ... [and] continues to provide money, weapons and training to select Iraqi Shia militants and terrorists despite pledges by senior Iranian officials to stop such support. The weapons include:

- Explosively Formed Penetrators (EFPs) with radio-controlled, remote arming and passive infrared detonators
- Improvised Explosive Devices (IED)
- Anti-aircraft weapons
- mortars
- 107 and 122 millimeter rockets
- rocket-propelled grenades and launchers
- explosives
- small arms.

[The IRGC-QF ...] also offers strategic and operational guidance to militias and terrorist groups to target U.S. Forces in Iraq and undermine U.S. interests. In addition to providing arms and support, IRGC-QF is responsible for training Iraqi insurgents in Iran, sometimes using Lebanese Hizballah instructors. Lebanese Hizballah provides insurgents with the training, tactics and technology to conduct kidnappings, small unit tactical operations and employ sophisticated IEDs.

72. These trends continued through the present day, throughout which period the IRGC used Hezbollah to provide the same weapons-related tactics, techniques, and procedures for its proxies throughout the Middle East, including Hamas, PIJ, and JAM. In April 2010, for example, DIA reported to Congress that "Iran provides Lebanese Hizballah and Palestinian terrorist groups" including "HAMAS" and "Palestinian Islamic Jihad . . . with funding, weapons,

and training to oppose Israel and disrupt the Middle East Peace Process.” In 2019, DIA reported to Congress:

The IRGC-QF maintains a wide and varied network of nonstate partners, proxies, and affiliates primarily in the Middle East. Iran provides a range of financial, political, training, and materiel support to these groups. Iran’s provision of military hardware has included small arms, ammunition, explosives, improvised explosive devices (IEDs), explosively formed penetrators (EFPs), vehicles, antitank guided missiles (ATGMs), man-portable air defense systems (MANPADS), artillery, rockets, UAVs, and some more-advanced systems, such as ASCMs and ballistic missiles, despite UN resolutions prohibiting Iranian arms exports. Tehran’s partners, proxies, and affiliates include Hizballah, Iraqi Shia militias, ... [and] Palestinian groups.

At all relevant times, the IRGC provided similar such weapons-related assistance to Hezbollah, Hamas, PIJ, and JAM.

73. From 2007 through the present, the IRGC was always a United States-designated terrorist organization. On October 25, 2007, the United States designated the IRGC-QF as a Specially Designated Global Terrorist (“SDGT”), designated the broader IRGC for non-proliferation-related sanctions, observed that the IRGC had seized a monopolistic share of Iran’s oil sector, emphasized that banks must follow the guidance of the Financial Action Task Force (“FATF”), and warned banks and companies contemplating doing business in Iran, or with Iranian counterparties, that the IRGC-QF used the money it obtained from commercial activities to finance IRGC-sponsored acts of terrorism targeting the United States and committed by IRGC proxies, including Hezbollah, Hamas, and JAM:

The U.S. Government is taking several major actions today to counter Iran’s ... support for terrorism by exposing Iranian banks, companies and individuals that have been involved in these dangerous activities and by cutting them off from the U.S. financial system.

Today, ... State designated under Executive Order 13382 [a] key Iranian entit[y] of proliferation concern: the Islamic Revolutionary Guard Corps (IRGC; aka Iranian Revolutionary Guard Corps) ...

The Treasury Department also designated the IRGC-Qods Force (IRGC-QF) under E.O. 13224 for providing material support to ... other terrorist organizations ...

Elements of the IRGC ... were listed in the Annexes to UN Security Council Resolutions 1737 and 1747. All UN Member States are required to freeze the assets of entities and individuals listed in the Annexes of those resolutions, as well as assets of entities owned or controlled by them, and to prevent funds or economic resources from being made available to them.

[FATF], the world's premier standard-setting body for countering terrorist financing and money laundering, recently highlighted the threat posed by Iran to the international financial system. FATF called on its members to advise institutions dealing with Iran to seriously weigh the risks resulting from Iran's failure to comply with international standards. Last week, ... Treasury ... issued a warning to U.S. banks setting forth the risks posed by Iran. ... Today's actions are consistent with this warning, and provide additional information to help financial institutions protect themselves from deceptive financial practices by Iranian entities and individuals engaged in or supporting ... terrorism. ...

#### **Proliferation Finance – Executive Order 13382 Designations**

E.O. 13382, signed by the President on June 29, 2005, is an authority aimed at freezing the assets of proliferators of weapons of mass destruction and their supporters, and at isolating them from the U.S. financial and commercial systems. Designations under the Order prohibit all transactions between the designees and any U.S. person, and freeze any assets the designees may have under U.S. jurisdiction.

The Islamic Revolutionary Guard Corps (IRGC): ... [T]he Islamic Revolutionary Guard Corps ... is composed of five branches (Ground Forces, Air Force, Navy, Basij militia, and Qods Force special operations) in addition to a counterintelligence directorate and representatives of the Supreme Leader. It runs prisons, and has numerous economic interests involving defense production, construction, and the oil industry. Several of the IRGC's leaders have been sanctioned under UN Security Council Resolution 1747. ...

IRGC-owned or -controlled companies: Treasury is designating the companies listed below under E.O. 13382 on the basis of their relationship to the IRGC. These entities are owned or controlled by the IRGC and its leaders. The IRGC has significant political and economic power in Iran, with ties to companies controlling billions of dollars in business and construction and a growing presence in Iran's financial and commercial sectors. Through its companies, the IRGC is involved in a diverse array of activities ... across the country. ...

#### **Support for Terrorism -- Executive Order 13224 Designations**

E.O. 13224 is an authority aimed at freezing the assets of terrorists and their supporters, and at isolating them from the U.S. financial and commercial systems. Designations under the E.O. prohibit all transactions between the designees and any U.S. person, and freeze any assets the designees may have under U.S. jurisdiction.

IRGC-Qods Force (IRGC-QF): The Qods Force, a branch of the Islamic Revolutionary Guard Corps (IRGC; aka Iranian Revolutionary Guard Corps), provides material support to the Taliban, Lebanese Hizballah, Hamas, Palestinian Islamic Jihad, and the Popular Front for the Liberation of Palestine-General Command (PFLP-GC).

The Qods Force is the Iranian regime's primary instrument for providing lethal support to the Taliban. The Qods Force provides weapons and financial support to the Taliban to support anti-U.S. and anti-Coalition activity in Afghanistan. Since at least 2006, Iran has arranged frequent shipments of small arms and associated ammunition, rocket propelled grenades, mortar rounds, 107mm rockets, plastic explosives, and probably man-portable defense systems to the Taliban. This support contravenes Chapter VII UN Security Council obligations. UN Security Council resolution 1267 established sanctions against the Taliban and UN Security Council resolutions 1333 and 1735 imposed arms embargoes against the Taliban. Through Qods Force material support to the Taliban, we believe Iran is seeking to inflict casualties on U.S. and NATO forces.

The Qods Force has had a long history of supporting Hizballah's military, paramilitary, and terrorist activities, providing it with guidance, funding, weapons, intelligence, and logistical support. The Qods Force operates training camps for Hizballah in Lebanon ... and has reportedly trained more than 3,000 Hizballah fighters at IRGC training facilities in Iran. The Qods Force provides roughly \$100 to \$200 million in funding a year to Hizballah and has assisted Hizballah in rearming in violation of UN Security Council Resolution 1701.

In addition, the Qods Force provides lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi'a militants who target and kill Coalition and Iraqi forces and innocent Iraqi civilians.

Treasury's October 25, 2007 IRGC sanctions rollout was a momentous event in world news, and received widespread media coverage.

74. On October 25, 2007, as part of the U.S. government's public rollout of its designation of the IRGC-QF as an SDGT and of the IRGC (in its entirety) for weapons proliferation, Secretary of the Treasury Henry M. Paulson, Jr. publicly warned, *inter alia*:

- a. “Today, we are taking additional steps to combat Iran’s dangerous conduct and to engage financial institutions worldwide to make the most informed decisions about those with whom they choose to do business. The Iranian regime’s ability to pursue ... missile programs in defiance of UN Security Council Resolutions depends on its access to the international commercial and financial systems. Iran also funnels hundreds of millions of dollars each year through the international financial system to terrorists.”
- b. “Iran’s banks aid this conduct, using a range of deceptive financial practices intended to evade even the most stringent risk-management controls.”
- c. “In dealing with Iran, it is nearly impossible to know one’s customer and be assured that one is not ... facilitating the regime’s reckless conduct.”
- d. “The recent warning by [FATF], the world’s premier standard-setting body for countering terrorist financing and money laundering, confirms the extraordinary risks that accompany doing business with Iran.”
- e. “We have been working closely and intensely with our international partners to prevent one of the world’s most dangerous regimes from developing the world’s most dangerous weapons. Part of that strategy involves denying supporters of Iran’s illicit conduct access to the international financial system; these actors should find no safe haven in the reputable world of finance and commerce.”
- f. “We are also designating the Islamic Revolutionary Guard Corps for proliferation activities and its Qods Force for providing material support to ... terrorist organizations. The IRGC is so deeply entrenched in Iran’s economy and commercial enterprises, it is increasingly likely that, if you are doing business with Iran, you are doing business with the IRGC.”
- g. “We call on responsible banks and companies around the world to terminate any business with ... all companies and entities of the IRGC.”
- h. “As awareness of Iran’s deceptive behavior has grown, many banks around the world have decided as a matter of prudence and integrity that Iran’s business is simply not worth the risk. It is plain and simple: reputable institutions do not want to be the bankers for this dangerous regime.”

75. On July 17, 2017, the United States announced new IRGC-related sanctions, and warned that “[t]he United States remains deeply concerned about” how the “Islamic Revolutionary Guard Corps (IRGC)” enabled “Iran’s malign activities across the Middle East,” because the IRGC “continues to support terrorist groups such as Hizballah” and “continue[d] to test and develop ballistic missiles.”

76. On August 2, 2017, Congress enacted, and the President signed, the Countering America's Adversaries Through Sanctions Act, which codified that "Congress makes the following findings: ... (2) The Iranian Revolutionary Guard Corps—Quds Force (in this section referred to as the "IRGC—QF") ... support[s] terrorist and insurgent groups [by] ... provid[ing] material, logistical assistance, training, and financial support to militants and terrorist operatives throughout the Middle East and South Asia"; and "(3) The IRGC, not just the IRGC—QF, is responsible for implementing Iran's international program of ... support for acts of international terrorism." § 105, 22 U.S.C. § 9404, Pub. L. No. 115-44, 131 Stat. 892 (2017). Moreover, "the IRGC, including the Quds Force ... [provided] support, including funding, lethal and nonlethal contributions, and training, ... to Hezbollah, Hamas, special groups in Iraq, ... and other violent groups across the Middle East." § 103(b)(5), 22 U.S.C. § 9402, Pub. L. No. 115-44, 131 Stat. 889 (2017).

77. On October 13, 2017, the United States designated the entirety of the IRGC as a SDGT, and stated, in part, as follows:

- a. Treasury: "OFAC ... designated [the] Islamic Revolutionary Guard Corps (IRGC) pursuant to the global terrorism Executive Order (E.O.) 13224 and consistent with the Countering America's Adversaries Through Sanctions Act. OFAC designated the IRGC today for its activities in support of the IRGC-Qods Force (IRGC-QF), which was designated pursuant to E.O. 13224 on October 25, 2007, for providing support to a number of terrorist groups, including Hizballah and Hamas .... The IRGC has provided material support to the IRGC-QF, including by providing training, personnel, and military equipment."
- b. Treasury: "'The IRGC has played a central role to Iran becoming the world's foremost state sponsor of terror. ... Treasury will continue using its authorities to disrupt the IRGC's destructive activities,' said Treasury Secretary Steven T. Mnuchin. 'We are designating the IRGC for providing support to the IRGC-QF, the key Iranian entity enabling ... the lethal activities of Hizballah, Hamas, and other terrorist groups. We urge the private sector to recognize that the IRGC permeates much of the Iranian economy, and those who transact with IRGC-controlled companies do so at great risk.'"

- c. Treasury: “The IRGC was designated today for the activities it undertakes to assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, the IRGC-QF.”
- d. White House: “[T]he Iranian regime continues to fuel ... terror ... throughout the Middle East and beyond” through “[t]he Revolutionary Guard[’s]” deployment as “the Iranian Supreme Leader’s corrupt personal terror force.”
- e. White House: “In Iraq and Afghanistan, groups supported by Iran have killed hundreds of American military personnel. The Iranian dictatorship’s aggression continues to this day. The regime remains the world’s leading state sponsor of terrorism, and provides assistance to ... Hezbollah, Hamas, and other terrorist networks.”
- f. White House: “The Revolutionary Guard ... has hijacked large portions of Iran’s economy and seized massive religious endowments [*i.e.*, bonyads or foundations, *e.g.*, the Foundation for the Oppressed] to fund ... terror abroad. This includes ... supplying proxies and partners with missiles and weapons to attack civilians in the region[] and even plotting to bomb a popular restaurant right here in Washington, D.C.”
- g. White House: “I am authorizing ... Treasury ... to further sanction the entire [IRGC] for its support for terrorism and to apply sanctions to its officials, agents, and affiliates.”

78. On October 16, 2017, Treasury Under Secretary Sigal Mandelker publicly confirmed how the entire IRGC was involved in supporting terrorist attacks in the Middle East committed by Hezbollah, Hamas, PIJ, and JAM:

- a. “[T]here are few more pressing national security concerns for the United States and the international community right now than the growing threat posed by ... [t]he Iranian regime,” which was “wreaking havoc on the Middle East and beyond” and providing “state support of terrorism” that was “second-to-none” by “financ[ing] and support[ing] Hizballah, Hamas, and ... Iraqi ... militant groups” by “seed[ing] these terror groups with increasingly destructive weapons as they try to establish footholds from Iran to Lebanon and Syria” and such “aid [was] primarily delivered by ... the IRGC[] and its Quds Force, which ... [existed as] vehicles to cultivate and support terrorists abroad.”
- b. “The IRGC has even threatened terrorist attacks right here in the United States, plotting the murder of Saudi Arabia’s Ambassador to the United States on American soil in 2011. Such an attack—if not thwarted by our terrific law enforcement and intelligence officers—would have not only killed a Saudi diplomat, but likely innocent bystanders here in Washington, DC.”
- c. “[The United States’s] Iran strategy ... is designed to neutralize Iran’s destabilizing influence and support for terrorists and militants. It includes four strategic objectives: First, we must neutralize Iran’s destabilizing activities and constrain Iran’s aggression, particularly its support for terrorism and militants with a focus on its activities in the

Middle East ...[,] includ[ing] its actions in Syria, which threatens Israel, and its support to terrorism through groups like Hizballah, Hamas, Iraqi Shia militant groups and others. Second, we must work to deny Iran and especially the IRGC funding for its malign activities, including its funding for terrorists and militant proxies ...”

- d. “On [October 13, 2017], OFAC designated the IRGC for support to terrorism under Executive Order 13224, consistent with section 105 of the Countering America’s Adversaries Through Sanctions Act passed in August. The President also authorized us to take additional action against the IRGC’s officials, agents, and affiliates later this month. The IRGC designation ... further increases the pressure on the IRGC. It also highlights the nefarious nature of the organization. Beyond being a proliferator of weapons and a supplier of militants and military equipment – actions for which it has been previously sanctioned by the United States – the IRGC has helped make Iran the world’s leading state sponsors of terrorism.”
- e. “The IRGC provides the organizational structure that allows them to export their militant extremism across the globe. It has been the Iranian regime’s main weapon in pursuit of its radical goals and is a lifeline for Hizballah, ... Shia militant groups in Iraq, and others. The IRGC’s control over large portions of the Iranian economy furthers its ability to support these groups and enrich its members. In order to deny the IRGC the resources and financing it needs to spread instability, we must and we have been engaging our allies and partners, including those in the private sector.”
- f. “[T]o deny the IRGC the resources and financing it needs to spread instability, we ... have been engaging ... the private sector. We have consistently raised concerns regarding the IRGC’s malign behavior, the IRGC’s level of involvement in the Iranian economy, and its lack of transparency. We have pointed out that the IRGC continues to be an integral part of the Iranian economy, including in the energy, construction, mining, and defense sectors. And as we have urged the private sector to recognize that the IRGC permeates much of the Iranian economy, we have told them that those who transact with IRGC-controlled entities do so at their own risk.”

79. On November 17, 2017, the U.S. government announced a wave of IRGC-related counterterrorism sanctions following on its announcement of the IRGC’s designation as an SDGT the month prior, and designated the IRGC Al-Ghadir Missile Command, IRGC Air Force, IRGC Aerospace Force Self Sufficiency Jihad Organization, and IRGC Research and Self Sufficiency Jihad Organization as SDGTs when it also designated the entire IRGC as an SDGT. In its November 17, 2017 rollout, OFAC’s director testified that: “OFAC has significantly increased the pressure on Iran and the [IRGC] for its malign activities. ... Just last month, consistent with the Countering America’s Adversaries Through Sanctions Act (CAATSA),

OFAC designated the IRGC itself under our counter-terrorism authority, Executive Order 13224.

... We have also consistently raised concerns with the private sector regarding the IRGC's malign behavior and its level of involvement in the Iranian economy. We have pointed out that the IRGC continues to be an integral part of the Iranian economy .... As we have urged the private sector to recognize that the IRGC permeates much of the Iranian economy, we have emphasized that those who transact with IRGC-controlled entities do so at their own risk."

80. On May 8, 2018, the United States announced new sanctions against the IRGC, confirming:

The Iranian regime is the leading state sponsor of terror. It exports dangerous missiles ... and supports terrorist proxies and militias such as Hezbollah [and] Hamas .... Over the years, [the IRGC] and its proxies have bombed American embassies and military installations, murdered hundreds of American servicemembers, and kidnapped, imprisoned, and tortured American citizens. The Iranian regime has funded [the IRGC's] long reign of chaos and terror by plundering the wealth of its own people.

81. On May 22, 2018, Treasury imposed counterterrorism sanctions "pursuant to E.O. 13224" against the IRGC-ASF, IRGC-ASF-AGMC, and their leaders to restrain "the IRGC's provision of missile-related support to" IRGC proxies in the Middle East.

82. On October 1, 2018, the United States published its counterterrorism strategy, confirming that the IRGC continued to seek to leverage its global networks of financiers, logisticians, and recruits, including persons in the United States, to sponsor acts of terrorism targeting the United States:

Iran remains the most prominent state sponsor of terrorism, supporting militant and terrorist groups across the Middle East and cultivating a network of operatives that pose a threat in the United States and globally. These groups, most notably Lebanese Hizballah (Hizballah), use terrorism ... in partnership with Iran to expand their influence in Iraq, Lebanon, [and] the Palestinian territories .... Hizballah fields powerful military and intelligence elements, possesses large stocks of sophisticated arms, and maintains extensive networks of operatives and sympathizers overseas, including individuals in the [United States] homeland.

83. On October 11, 2018, Treasury’s Financial Crimes Enforcement Network (“FinCEN”) published its *Advisory On The Iranian Regime’s Illicit And Malign Activities And Attempts To Exploit The Financial System*, in which FinCEN warned multinational companies and financial institutions, including virtual currency exchanges like Binance, that whenever a company or bank enables the IRGC’s “Abuse of the International Financial System ... to access the financial system through covert means and to further [the IRGC’s] malign activities [by] ... misusing banks and exchange houses, operating procurement networks that utilize front or shell companies, exploiting commercial shipping, and masking illicit transactions using senior officials, ... *[o]ften, these efforts serve to fund the regime’s nefarious activities, including providing funds to the Islamic Revolutionary Guard Corps (IRGC) and its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), as well to Lebanese Hizballah, ... and other [IRGC proxy] terrorist groups.*” (Emphasis added.) Treasury’s rollout confirmed, *inter alia*:

- a. “[T]he Iranian regime has masked illicit transactions using senior officials of the CBI, who used their official capacity to procure hard currency and conduct transactions for the benefit of the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) and its terrorist proxy group, Lebanese Hizballah. Accordingly, financial institutions are advised to exercise appropriate due diligence when dealing with transactions involving exchange houses that may have exposure to the Iranian regime and/or designated Iranian persons, and the advisory details examples of exchange house-related schemes. Iran-related actors use front and shell companies around the world in procurement networks through which the Iranian regime has gained goods and services related to currency counterfeiting, dual-use equipment, and the commercial aviation industry.”
- b. “In order to help financial institutions identify deceptive activity potentially linked to the Iranian regime, FinCEN has included red flags in its advisory. For example, CBI officials’ routing transactions to personal accounts rather than central bank or government-owned accounts, and individuals or entities with no central bank or government affiliation withdrawing funds from such accounts, may be a red flag for financial institutions to investigate. Similarly, wire transfers or deposits that do not contain any information on the source of funds, contain incomplete information about the source of funds, do not match the customer’s line of business, or that involve jurisdictions where there is a higher risk of dealing with entities linked to the Iranian regime may be

red flag indicators of illicit Iranian attempts to gain access to the U.S. financial system or evade sanctions.”

84. On November 5, 2018, the United States announced a massive new raft of sanctions against the IRGC, as well as the full reimposition of all sanctions that had been lifted under the Obama-era Iran nuclear deal, and stated, *inter alia*, as follows:

- a. “Today, in its largest ever single-day action targeting the Iranian regime, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) sanctioned more than 700 individuals, entities, aircraft, and vessels. This action is a critical part of the reimposition of the remaining U.S. nuclear-related sanctions that were lifted or waived in connection with the Joint Comprehensive Plan of Action (JCPOA). OFAC’s action is designed to disrupt the Iranian regime’s ability to fund its broad range of malign activities, and places unprecedented financial pressure on the Iranian regime to negotiate a comprehensive deal that will permanently prevent Iran from acquiring a nuclear weapon, cease Iran’s development of ballistic missiles, and end Iran’s broad range of malign activities. This brings to more than 900 the number of Iran-related targets sanctioned under this Administration in less than two years, marking the highest-ever level of U.S. economic pressure on Iran.”
- b. “‘Treasury’s imposition of unprecedented financial pressure on Iran should make clear to the Iranian regime that they will face mounting financial isolation and economic stagnation until they fundamentally change their destabilizing behavior. Iran’s leaders must cease support for terrorism, stop proliferating ballistic missiles, end destructive regional activities, and abandon their nuclear ambitions immediately if they seek a path to sanctions relief,’ said Treasury Secretary Steven Mnuchin. ‘The maximum pressure exerted by the United States is only going to mount from here. We are intent on making sure the Iranian regime stops siphoning its hard currency reserves into corrupt investments and the hands of terrorists.’”
- c. “Today marks the largest single-day OFAC action targeting the Iranian regime’s abuse of Iran’s banking sector to fund its destabilizing activities. For example, the Iranian regime has funneled the equivalent of billions of dollars for the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) through the banking sector. The action targets, in particular, Iranian banks that have provided support to, or are owned or controlled by, persons designated in connection with the Iranian regime’s support to international terrorism, proliferation of weapons of mass destruction (WMD) or their means of delivery, and human rights abuses. Some of the banks designated today have served as financial conduits for the IRGC-QF, the Ministry of Defense and Armed Forces Logistics (MODAFL), the Islamic Republic of Iran Broadcasting (IRIB), the Martyrs Foundation, Mahan Air, and Iran’s Law Enforcement Forces (LEF) — all entities that remained designated throughout the JCPOA.”
- d. “‘As the Iranian people suffer from fiscal mismanagement and a plummeting rial, the Iranian regime abuses the country’s banking system to enrich its elite and finance

repressive state institutions. The IRGC and other destabilizing entities leverage their access to the global financial system to fund proxies fighting in Syria, Iraq, and Yemen, subsidize the proliferation of WMD or their means of delivery, and arm those who abuse the human rights of Iranian citizens,’ said Treasury Under Secretary Sigal Mandelker. ‘This action is aimed at cutting off Iranian banks that facilitate Iran’s domestic repression and foreign adventurism from the international financial system, and will highlight for the world the true nature of the regime’s abuse of its domestic banking system.’”

- e. “Today, more than 70 Iran-linked financial institutions and their foreign and domestic subsidiaries were designated or ... placed on the SDN List.”

85. As part of the same rollout on November 5, 2018, Treasury Secretary Mnuchin warned, *inter alia*:

- a. “[November 5, 2018] marks the heaviest economic pressure ever applied by the US against the Iranian regime. This effort is but a part of the US government’s strategy to change the behaviour of Ayatollah Khamenei, and Iran’s Revolutionary Guard Corps. In the early hours of Monday, the Treasury department will complete its full snapback of sanctions on Iran, targeting the energy, shipping and banking sectors, among others. We are also adding back hundreds of targets previously removed from sanctions lists, as well as more than 300 new targets.”
- b. “The hope and goal [of the Nuclear Deal] was that Iran’s leaders would use this influx of investment [under the Nuclear Deal] to lift up their people. Instead, the regime did what it always does: poured money into supporting terrorism, fomenting violence and promoting regional instability. From its support of ... the Houthis in Yemen, to missile attacks on its neighbours, the Iranian regime actually grew more aggressive.”
- c. “We will impose sanctions on foreign financial institutions that knowingly engage in certain significant transactions with the Central Bank of Iran and designated Iranian financial institutions. We know that these transactions are critical to a network that fuels the radical ambitions of the IRGC and its Quds Force, which siphons millions of dollars away from legitimate activities to fund terrorism across the region. These powerful sanctions are designed to cut off all sources of revenue to a regime that continues to fund terror ... [by, *inter alia*, supporting] networks that recruit and train child soldiers [and] fund Hizbollah ...”.
- d. “The Treasury will strictly enforce our sanctions. We will not tolerate banks, companies or other entities that seek to circumvent our actions. We will view them as complicit in funding Iran’s malign ambitions.”

86. On March 26, 2019, Treasury designated the Iranian Ministry of Defense, Armed Forces, and Logistics as an agent for both the Qods Force and the IRGC-QF’s terrorist proxies.

87. On April 8, 2019, the U.S. announced its intention to formally designate the entire IRGC—including the regular IRGC, the Qods Force, and the Basij—as an FTO, which the U.S. did on April 15, 2019. During the rollout, U.S. officials warned, in part, as follows:

- a. President Donald J. Trump, April 2019: “Today, I am formally announcing my Administration’s plan to designate Iran’s Islamic Revolutionary Guard Corps (IRGC), including its Qods Force, as a Foreign Terrorist Organization (FTO) under Section 219 of the Immigration and Nationality Act. This unprecedented step, led by the Department of State, recognizes the reality that Iran is not only a State Sponsor of Terrorism, but that the IRGC actively participates in, finances, and promotes terrorism as a tool of statecraft. The IRGC is the Iranian government’s primary means of directing and implementing its global terrorist campaign. This designation will be the first time that the United States has ever named a part of another government as a FTO. It underscores the fact that Iran’s actions are fundamentally different from those of other governments. ... If you are doing business with the IRGC, you will be bankrolling terrorism.”
- b. Secretary of State Michael R. Pompeo, April 2019: “I’m here to make an important foreign policy announcement concerning the Islamic Republic of Iran. Today the United States is continuing to build its maximum pressure campaign against the Iranian regime. I am announcing our intent to designate the Islamic Revolutionary Guard Corps, including its Qods Force, as a foreign terrorist organization in accordance with Section 219 of the Immigration and Nationality Act. ... This is the first time that the United States has designated a part of another government as an FTO. We’re doing because the Iranian regime’s use of terrorism as a tool of statecraft makes it fundamentally different from any other government. This historic step will deprive the world’s leading state sponsor of terror the financial means to spread misery and death around the world. ... Our [IRGC FTO] designation makes clear to the world that Iranian regime not only supports terrorist groups, but engages in terrorism itself. This designation also brings unprecedented pressure on figures who lead the regime’s terror campaign, individuals like Qasem Soleimani. He is the commander of the Qods Force and oversees Iran’s forces deployed to advance the Islamic Revolution through terrorism and other forms of violence. He doles out the regime’s profits to terrorist groups across the region and around the world. ... [T]he mission of this [U.S.] designation [of the IRGC as a Foreign Terrorist Organization is] ... to achieve the outcomes that we laid out back in May [2018] to ... [stop the IRGC from] ... risking American lives each and every day.”
- c. State, April 2019: “The IRGC – primarily through its Qods Force – is the primary arm of the Iranian government that carries out and directs Tehran’s dangerous and destabilizing global terrorist campaign. The IRGC provides funding, equipment, training and logistical support to a broad range of terrorist and militant organizations, totaling approximately one billion dollars annually in assistance. The IRGC has also been directly involved in terrorist plotting and related activity in many countries ... The IRGC is integrally woven into the Iranian economy, operating front companies and institutions around the world that engage in both licit and illicit business activity. The profits from what appear to be legitimate business deals could end up ... supporting Iran’s terrorist agenda.”

88. On April 15, 2019, the United States designated the entire IRGC, including the regular IRGC, the Qods Force, and the Basij, as an FTO for, *inter alia*, “provid[ing] financial and other material support, training, technology transfer, advanced conventional weapons, guidance, or direction to a broad range of terrorist organizations, including Hizballah, Palestinian terrorist groups like Hamas and Palestinian Islamic Jihad, Kata’ib Hizballah in Iraq, ... and other terrorist group[s]....” In support, State concluded that the IRGC “has engaged in terrorist activity since its inception 40 years ago,” that “its support for terrorism is foundational and institutional,” that it “has killed U.S. citizens,” and that it “has the greatest role among Iran’s actors in directing and carrying out a global terrorist campaign.” Announcing the designation, Secretary of State Pompeo emphasized that the IRGC “plans, organizes, and executes terror campaigns all around the world,” and that the “IRGC institutionalized terrorism shortly after its inception, directing horrific attacks . . . alongside the terror group it midwived, Lebanese Hizballah.” Secretary Pompeo described the designation as “simply recognizing a basic reality,” placing the IRGC in “its rightful place on the same list as terror groups it sponsors.”

89. As State reported to Congress in 2020, its “designat[ion]” of the “IRGC as an FTO in April 2019” was a “historic action” and “unprecedented step,” which “reflected the Iranian regime’s unique place among the governments of the world in its use of terrorism as a central tool of its statecraft.”

90. On October 25, 2019, the U.S. government designated Iran as a region of primary concern for purposes of counter-terrorist finance and anti-money laundering. It did so because FinCEN found, in sum and substance, that it was impossible to transact business in Iran, or with Iran-related parties, without recklessly running the risk of facilitating IRGC-sponsored acts of terrorism committed by the IRGC or IRGC proxies like Hezbollah, Hamas, and JAM.

91. On January 14, 2020, President Trump implemented Executive Order 13,902, which imposed additional counterterrorism sanctions on the IRGC, and found, *inter alia*:

- a. “[The President] find[s] that Iran continues to be the world’s leading sponsor of terrorism and that Iran has threatened United States military assets and civilians through the use of military force and support to Iranian-backed militia groups. It remains the policy of the United States to ...counter the totality of Iran’s malign influence in the region. In furtherance of these objectives, it is the policy of the United States to deny the Iranian government revenues, including revenues derived from the export of products from key sectors of Iran’s economy, that may be used to fund and support its ... terrorism and terrorist proxy networks ....”
- b. “[The President] hereby determine[s] that the making of donations of the types of articles specified in section 203(b)(2) of IEEPA (50 U.S.C. 1702(b)(2)) by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to section 1 of this order would seriously impair the President’s ability to deal with the national emergency declared in Executive Order 12957 [*i.e.*, the IRGC’s sponsorship of acts of terrorism targeting the United States].”

92. On March 26, 2020, Treasury announced new counterterrorism sanctions against the IRGC pursuant to E.O. 13,324 and reported findings as follows:

- a. “OFAC ... today designated 20 Iran- and Iraq-based front companies, senior officials, and business associates that provide support to or act for or on behalf of the Islamic Revolutionary Guards Corps-Qods Force (IRGC-QF) in addition to transferring lethal aid to Iranian-backed terrorist militias in Iraq such as Kata’ib Hizballah (KH) and Asa’ib Ahl al-Haq (AAH). Among other malign activities, these entities and individuals perpetrated or supported: smuggling through the Iraqi port of Umm Qasr; money laundering through Iraqi front companies; selling Iranian oil to the Syrian regime; smuggling weapons to Iraq ...; promoting propaganda efforts in Iraq on behalf of the IRGC-QF and its terrorist militias .... The terrorist militias supported by the Iranian regime such as KH and AAH have continued to engage in attacks on U.S. and Coalition forces in Iraq.”
- b. “‘Iran employs a web of front companies to fund terrorist groups across the region, siphoning resources away from the Iranian people and prioritizing terrorist proxies over the basic needs of its people,’ said Treasury Secretary Steven T. Mnuchin.”

93. On May 1, 2020, the United States announced new counterterrorism sanctions against the IRGC and confirmed that “senior officials of [the] Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF)” were “involved in IRGC-QF efforts to generate revenue and smuggle weapons abroad” through an IRGC front “company owned, controlled, or directed by”

an IRGC member, thereby “violat[ing] [U.S.] sanctions and money laundering laws” by committing “crimes” that caused valuable “assets” to flow to “a foreign terrorist organization.”

94. On June 1, 2023, the United States imposed counterterrorism sanctions, pursuant to E.O. 13224, against numerous members and affiliates of the IRGC-QF and IRGC-IO based on Treasury’s determination that such persons “participated in a series of terrorist plots including assassination plots targeting former United States government officials, dual U.S. and Iranian nationals, and Iranian dissidents.” With respect to the IRGC-QF, Treasury “target[ed] three Iran- and Türkiye-based individuals and a company affiliated with the IRGC-QF ... who have been involved in plotting [such] external lethal operations against [U.S. national] civilians including journalists and activists.” In the same finding, Treasury also observed: “Treasury has consistently acted to address external terrorist plotting by the IRGC-QF and Iran’s intelligence service [*i.e.*, IRGC-IO], notably: the October 2011 designation of senior IRGC-QF officials involved in an Iranian plot to assassinate the Saudi Arabian Ambassador to the United States; the December 2020 designation of an individual involved in the IRGC-QF’s efforts to plan and execute operations in the Middle East and the United States; and the September 2021 designation of Iranian intelligence [IRGC-IO] operatives who targeted a U.S. citizen in the United States and Iranian dissidents in other countries as part of a wide-ranging campaign to silence critics of the Iranian government.”

95. Iran was without peer as a nation in which a transnational terrorist group operated in support of the government’s terrorist objectives.<sup>6</sup> United States policy therefore “simply

---

<sup>6</sup> Indeed, Iran and Afghanistan are the only two nations in which a transnational terrorist group currently exercises sovereignty, joined only by the Islamic State of Iraq and Syria (“ISIS” during its caliphate era from 2014-2017. In Afghanistan, that terrorist group is the Taliban (a Specially Designated Global Terrorist), including its Haqqani Network (a Foreign Terrorist Organization),

recogniz[es]” the “basic reality” that “[t]he IRGC” has a “rightful place on the same [terrorist] list as terror groups its supports: Lebanese Hizballah, Palestinian Islamic Jihad, Hamas, Kata’ib Hizballah, among others, all of which are already designated as foreign terrorist organizations.”

### **3. The IRGC and Supreme Leader’s Office Seized Key Iranian Economic Sectors to Finance, Arm, and Logistically Support IRGC-Sponsored Terrorist Attacks**

96. Beginning no later than 2007, the IRGC, Supreme Leader’s Office, and their associated foundations and fronts, notoriously seized and controlled well over half of the entire Iranian economy; some estimates ranged as high as 85%. Indeed, the U.S. government has concluded similarly. In 2021, for example, Treasury observed that IRGC- and Supreme Leader-related entities were collectively “said to control more than half of the Iranian economy.”

97. Between 2005 and 2009, using fronts they controlled, the IRGC and SLO orchestrated a monopolistic takeover of key components of Iran’s economy. Per a DoD analysis published on October 12, 2011:

The IRGC’s expansion beyond the roles and tasks traditionally associated with military or security services is most pronounced in its dominant role in Iran’s economy. Speaking at the change of command at the *Khatam ol-Anbia* Base Complex, IRGC commander [Mohammad Ali] Jafari bluntly summarized his position, “The IRGC must play a leading role in the nation’s economic fronts.” Referencing the IRGC’s role in the Iran-Iraq war, Jafari further rationalized the IRGC’s economic responsibilities, “The IRGC actually goes into areas of activity the other sectors cannot do, as in [Iran-Iraq] war where ... the IRGC had the duty to go on the battlefield with all its being. We are doing the same thing today in economic areas.” ...

Through [the IRGC’s] complex network of foundations and their subsidiary banks, assisted by generous subsidies, the IRGC has diligently expanded its business holdings at a deep discount. The true private sector only gained 19% of the “privatized” public assets, while the cooperatives consumed 68% of the resources. The IRGC has systematically militarized rather than privatized the Iranian economy.

---

which have asserted sovereignty over the entire country since 2021. In Iran, that terrorist group is the IRGC, including its subordinate parts, the Qods Force and the IRGC’s Lebanese Hezbollah Division, which have asserted sovereignty since 1979.

98. The IRGC’s ability to leverage its control of entire sectors of Iran’s economy directly funded IRGC-sponsored attacks committed by Hezbollah, Hamas, PIJ, JAM, and other IRGC proxies. On October 6, 2009, for example, Treasury Under Secretary Levey testified before Congress that:

In the name of privatization, the IRGC has taken over broad swaths of the Iranian economy. . . . Furthermore, the IRGC seeks to monopolize black-market trade of popular items, funneling the proceeds from these transactions through a patronage system and using them to help subsidize . . . support for terrorist groups.

On June 22, 2010, Treasury Under Secretary Levey testified before Congress that “the Revolutionary Guards . . . has provided material support to . . . Lebanese Hizballah, Hamas, Palestinian Islamic Jihad, and others,” the needed funding for which compelled the IRGC to “assume[] control over broad areas of the Iranian economy.”

99. Terrorism scholars also concluded that the IRGC seized monopolies during this period to support its proxies’ acts of terrorism.

100. The Supreme Leader and IRGC strategy for monopolization focused on key sectors: they did not seek to control the entire economy, just those sectors that were inextricably connected to the IRGC’s ability to sponsor terrorism. Consequently, beginning in or around 2007, the IRGC notoriously exercised a monopoly over certain IRGC “exclusive sectors” of Iran’s economy, including the energy, construction, import/export, and communications sectors.

101. Despite the substantial nature of the IRGC’s and SLO’s involvement throughout Iran’s economy from 2007 through present, Plaintiffs do not allege that the IRGC monopolized every—or even most—segments of Iran’s economy. While the IRGC and SLO had substantial interests in most Iranian economic sectors, they only exercised a monopoly in certain sectors, including the sectors alleged herein.

**a. The Sanctions Evasion Sector**

102. In Iran, sanctions evasion was an industrial sector with dedicated practitioners, firms, strategies and the like and primarily comprised three sub-sectors: (1) the black market; (2) smuggling and port operations; and (3) transnational shipping and logistics. The SLO and IRGC exercised a monopoly over Iran’s sanctions evasion sector, as Plaintiffs define it herein.

103. The United States has formally confirmed that the IRGC exercised a monopoly over Iran’s inextricably linked sanctions evasion, smuggling, and black market sectors, and used such monopoly to fund terrorist attacks by its proxies. In April 2011, for example, State reported to Congress that the “IRGC is . . . widely considered to control the vast majority of [Iran’s] underground and black market economy.” As RAND scholars warned in 2009, “the IRGC” exercised “control of Iran’s shadow economy” including “the illicit smuggling networks.”

**b. The Financial Sector**

104. By late 2007, the Supreme Leader and IRGC had seized a monopoly in Iran’s financial sector, which comprised Iranian banks, currency exchanges, and hawalas, operationalized through, *inter alia*, the SLO and the Central Bank of Iran. These entities, collectively, owned and/or exercised direct or indirect control over all banks, currency exchanges, and hawalas in Iran.

105. The United States has formally confirmed that the Iranian regime exercised a monopoly over Iran’s banks and used that monopoly to fund terrorist attacks by IRGC proxies. On August 6, 2018, for example, President Trump signed Executive Order 13,846 based upon the Executive branch’s finding that U.S. dollar-denominated transactions with any person supervised by “the Central Bank of Iran”—Iran’s financial regulator, which controlled all Iranian banks—directly enabled “threats posed by Iran, including Iran’s . . . network and campaign of regional aggression, its support for terrorist groups, and the malign activities of the Islamic

Revolutionary Guard Corps and its surrogates.” On September 20, 2019, Treasury sanctioned the Central Bank of Iran, and confirmed its findings that the Qods Force and Hezbollah controlled the Central Bank of Iran and used it to finance their attacks as well as those of their proxies, including Hezbollah, Hamas, PIJ, and JAM:

Iran’s Central Bank has provided billions of dollars to the Islamic Revolutionary Guards Corps (IRGC), its Qods Force (IRGC-QF) and its terrorist proxy, Hizballah. ...

“Treasury’s action targets a crucial funding mechanism that the Iranian regime uses to support its terrorist network, including the Qods Force, Hizballah, and other militants that spread terror and destabilize the region....”...

**CENTRAL BANK OF IRAN FUNDS THE IRGC, ITS QODS FORCE AND HIZBALLAH**

Today’s action targets the CBI for its financial support to the IRGC-QF and Hizballah.... Since at least 2016, the IRGC-QF has received the vast majority of its foreign currency from the CBI and senior CBI officials have worked directly with the IRGC-QF to facilitate CBI’s financial support to the IRGC-QF. In 2017, the IRGC-QF oversaw the transfer of tens of millions of euros to Iraq from the CBI. Then-Governor of the CBI Valiollah Seif directed the transfer. ...

CBI has [] coordinated with the IRGC-QF to transfer funds to Hizballah.

OFAC is designating the CBI today for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to, the IRGC-QF and Hizballah.

106. Beginning in at least 2007, the SLO and IRGC continuously, and notoriously, exercised their monopoly over all Iran-related bank, currency exchange, and hawala transactions.

**c. The Import/Export Sector**

107. By late 2007, the Supreme Leader and IRGC had seized a monopoly in Iran’s import/export sector, which was comprised of Iranian importers and exporters who typically had affiliated entities outside of Iran, operationalized through, *inter alia*, the SLO and the Central Bank of Iran. These entities, collectively, owned and/or exercised direct or indirect control over all banks, currency exchanges, and hawalas in Iran.

108. Reports and statements published by the United States, Iranian regime, Iranian opposition, media, terrorism scholars, and NGOs warned that import- and export-related

transactions concerning Iranian counterparties, deals, or projects supported IRGC-sponsored terrorist violence committed by IRGC proxies, because of the IRGC's and SLO's assumption of a monopoly over Iran's import/export sector. Such warnings included, but were not limited to:

- a. Economist, February 2, 2013: "[T]he Revolutionary Guard ... enjoys ... a virtual monopoly over imports."
- b. Dr. Michael Rubin, April 19, 2016: "IRGC ... maintains a stranglehold over trade and the economy and so has become the chief if not sole beneficiary from the hard currency now flowing into Iran."
- c. Perviz S. Khazai (National Council of Resistance of Iran), April 22, 2019: "[IRGC] members ... loot[] ... [Iran]'s wealth to support their policy of exporting the 'Islamic revolution' ... in the Middle East. ... The IRGC ... has monopolized the lion's share of the Iranian economy since 2005 ... [including] ... import and export ... [and] ... is the financier and gunsmith of Hezbollah ... [and] barbaric militias in Iraq ...."
- d. Eurasia Review, August 15, 2020: "The drop in foreign currency revenue [shows] ... the plundering [of Iranian wealth] by corrupt bands affiliated to the ... IRGC ... and Khamenei himself. ... This mafia band [comprised of] ... the IRGC and The Executive Headquarters of Imam [*i.e.*, the SLO], which belongs to Khamenei, is clinging on to Iran's import and export trade like an octopus, with exclusive control over it, causing immense corruption. ... The wealth of bodies and institutions under the control of Iran's Supreme Leader, Ali Khamenei, is estimated at hundreds of billions of dollars. Today the majority of banks, industries, mines, communication enterprises, and financial institutions are under the exclusive ownership of Khamenei and the [IRGC]. Each year tens of billions of dollars are drained out of the country through the mullahs' and IRGC's corruption and looting, being spent on the regime's terrorism and its proxies in Iraq, Syria, ... and Lebanon. This has gone so far that the United States has issued an ultimatum that it will close its embassy in Baghdad unless the regime's proxies are brought to account for their consecutive attacks on [U.S.] embassies and convoys."
- e. National Council of Resistance of Iran, April 2022: "When it comes to ... domestic and foreign commerce ... Khamenei's office (along with the IRGC) has taken control of virtually everything that matters. ... [T]he astronomical profits ... end[] up funding ... IRGC ... terror operations in ... Iraq ... and ... around the world."

109. From at least 2007, the SLO and IRGC continuously, and notoriously, exercised their monopoly over all Iran-related import/export companies.

**d. The Communications Sector**

110. The SLO and IRGC began their seizure of the communications sector when it seized control of Irancell—Iran’s most important internet and telecoms company—in 2005. The SLO and IRGC completed their seizure of the communications sector in 2009, when they collaborated to help the IRGC purchase the Telecommunications Company of Iran. By 2009, the Supreme Leader and IRGC had seized a monopoly in Iran’s communications sector, which comprised Iranian telecoms, internet, social media, and computing, and communications technologies firms. These entities, collectively, owned and/or exercised direct or indirect control over all communications companies in Iran.

111. Beginning no later than 2009, reports and statements published by the United States, Iranian regime, Iranian opposition, media, terrorism scholars, and NGOs alerted Defendants that communications-related transactions (including landline and mobile telecoms, internet, computing, social media, and associated technologies) concerning Iranian counterparties, deals, or projects supported IRGC-sponsored terrorist violence committed by IRGC proxies given the IRGC’s assumption of a monopoly over the Iranian communications sector. Such warnings included, but were not limited to:

- a. Ali Alfoneh (American Enterprise Institute), October 22, 2007: “The IRGC rooted its rhetoric on [seizing telecoms companies] in national security. ... the IRGC expects to maintain its dominant position not only on the battlefield, but in civilian sectors as well. ... Because some of the Iranian economy’s most advanced technological undertakings occur under the aegis of the IRGC and within the framework of the Iranian arms industry, the IRGC can monopolize the transfer and adaptation of high technology to civilian applications ... The homepage of [IEI] ... display[s] many consumer goods produced by the arms industry for sale in the Iranian market. The list includes personal computers, scanners, telephone sets and intercoms, mobile phones, and telephone sim cards. These purchases support ... IRGC operations ....”
- b. APS Diplomat News Service, November 23, 2009: “[T]he IRGC now monopolises Iran’s huge communications sector.”

- c. UPI, November 24, 2009: “[A] company tied to the Revolutionary Guards acquired a majority share in the nation’s telecommunications monopoly, essentially giving the [IRGC] control of Iran’s land lines, Internet providers and cellphone companies.”
- d. Guardian, November 25, 2009: “[U]nofficial spokesman for the opposition Green Movement ... Mohsen Makhmalbaf ... called for ‘smart’ sanctions targeting the Islamic Revolutionary Guard Corps and their extensive business interests – including a communications monopoly – that are often described as constituting a parallel economy. ‘The Revolutionary Guards are terrorists. They are in Iraq ... and Lebanon.’”
- e. Dr. Monika Gill, October 2020: “[W]hilst the Guard relied on the communications economy to propagate their ideology, they also acquired and monopolised communications infrastructure as a source of capital gain. The Guard’s involvement with the communications economy moved beyond the projection of revolutionary ideology, becoming equally a matter of realpolitik and of accruing military capital.”

112. Beginning in at least 2007, the SLO and IRGC continuously, and notoriously, exercised their monopoly over all Iran-related telecoms, internet, social media, computing, and communications technology-related transactions.

## **B. Hezbollah**

113. In 1982, the IRGC founded Hezbollah, and it has served as the IRGC’s most important terrorist proxy ever since. From 1982 through 1989, Hezbollah members swore their loyalty to Ayatollah Khomeini. Ever since, Hezbollah members have sworn their loyalty to Ayatollah Khamenei.

114. Hezbollah, like its IRGC patrons, viewed attacks targeting Israel and Israeli civilians as inextricably connected to its efforts to target the *United States* to withdraw from the Middle East. Among other reasons, Hezbollah believed that the United States controlled Israel, that the United States could be punished, in effect, through attacks against its ally, and that—as Khomeini and Khamenei both emphasized—Israel comprised the “Little Satan” to the America’s “Great Satan.”

115. Hezbollah General Secretary Hassan Nasrallah has publicly admitted, “Hezbollah’s budget, its income, its expenses, everything it eats and drinks, its weapons and

rockets, come from the Islamic Republic of Iran.” As the U.N. Security Council’s panel of experts reported on December 30, 2016: “In a televised speech broadcast by Al-Manar television on 24 June 2016, the Secretary-General of Hizbullah [Hassan Nasrallah] stated that the budget of Hizbullah, its salaries, expenses, weapons and missiles all came from the Islamic Republic of Iran. ... [T]hat statement ... suggests that transfers of arms and related materiel from the Islamic Republic of Iran to Hizbullah may have been undertaken.”

116. Senior U.S. officials confirmed that the Iranian regime, including the IRGC, was vital to financing Hezbollah’s attacks. On September 29, 2006, for example, Frank C. Urbancic, Principal Deputy Coordinator at State, testified before Congress as follows:

Iran is the ‘central banker’ of terrorism and a primary funding source for Hizballah. Because money is a terrorist group’s oxygen, attacking terrorist financing is an essential element to combating terrorism. In that regard, we have made progress in impeding Iran’s financial support for Hizballah and in undermining Hizballah’s own financial network. ...

The USG has long assessed that Iran provides technological, operational, and financial support and guidance to Lebanese Hizballah. The Iranian regime has for 27 years used its connections and influence with terrorist groups to combat U.S. interests it perceives as at odds with its own, and Hizballah has acted as a willing partner.

117. On May 27, 2009, Treasury imposed sanctions targeting Hezbollah and confirmed the Iranian regime’s, including the IRGC’s, continued key role in financing Hezbollah attacks:

Treasury [] designated ... supporters of ... Hizballah ..., under E.O. 13224. E.O. 13224 targets terrorists and those providing support to terrorists or acts of terrorism by ... prohibiting U.S. persons from engaging in any transactions with them. “We will continue to take steps to protect the financial system from the threat posed by Hizballah and those who support it,” said Under Secretary for Terrorism ... Stuart Levey. ... Iran ... provide[s] significant support to Hizballah, giving money, weapons and training to the terrorist organization. In turn, Hizballah is closely allied with and has an allegiance to [Iran]. Iran is Hizballah’s main source of weapons and uses its Islamic Revolutionary Guard Corps to train Hizballah operatives in Lebanon and Iran. Iran provides hundreds of millions of dollars per year to Hizballah.

118. The IRGC and the SLO provided most of Hezbollah's budget, and directly financed Hezbollah attacks through a range of vehicles, including salary and bonus payment to Hezbollah leaders and attack cells, bounties for successful attacks, and martyr payments to the families of dead Hezbollah terrorists. The Iranian regime funded acts of terrorism committed by Hezbollah through an array of channels.

119. Hezbollah ordinarily acted as the IRGC's interlocutor with its terrorist proxies, including Hamas and PIJ in Israel and JAM in Iraq. Hezbollah provided expert training, technical assistance, and in-country support, often through joint cells co-located with Hamas and PIJ (in, *inter alia*, Gaza, Lebanon, and Syria) and with JAM (in, *inter alia*, Baghdad and Basra).

120. Hezbollah pioneered several signature attacks, including kidnapping, roadside bomb attacks using sophisticated devices known as explosively formed penetrators, and rocket attacks using 107mm rockets. The IRGC relied upon Hezbollah's experience and technical expertise to train other proxies, including Hamas, PIJ, and JAM, with respect to how to effectively conduct such attacks.

121. Hezbollah played a vital planning role for IRGC proxies, including Hamas and JAM. Hezbollah had vast experience that the other groups lacked, and it drew on such experience to help such groups devise specific attack types, locations, and tactics. For example, Hezbollah taught Hamas, PIJ, and JAM how to effectively kidnap targets.

122. Hezbollah was designated by the U.S. Secretary of State as an FTO in or about October 1997, and it has remained so-designated ever since.

### **C. Hamas**

123. Hamas established itself in or about 1987 as a violent, global, Sunni Islamist group dedicated to destroying Israel and killing every Jewish person there. From its inception,

Hamas's stated purpose has been to create an Islamic Palestinian state throughout Israel by eliminating the State of Israel through violent holy war.

124. Hamas has not only directed its violence and terrorism against Israeli targets in furtherance of that goal; Hamas's leaders have also attacked and assailed the United States and American citizens in retaliation for and in an effort to weaken U.S. support for Israel.

125. Hamas's operations arm, the Izz al-Din al-Qassam Brigades, has conducted numerous terrorist attacks in both Israel and the Palestinian territories since the 1990s.

126. Hamas has murdered and injured dozens of Americans as part of its campaign of violence and terror.

127. Hamas regularly violates the laws of war when it commits its barbaric attacks. As Hamas scholar Jonathan Schanzer observed in 2021: "Hamas was a brutal enemy" that routinely engaged in "'extra-judicial and willful killing,' including incidents in which Hamas fighters pushed [captured rivals] off tall buildings."

128. Hamas was designated by the U.S. Secretary of State as an FTO on or about October 8, 1997, and it has remained so-designated ever since. Hamas has been listed as an SDGT since 2001.

129. The Islamic Republic of Iran—particularly the IRGC and its Qods Force—has supported, supplied, and trained Hamas terrorists. Throughout that relationship, Hamas has played a significant role in the IRGC's regional and global campaign of supporting terrorism to damage, weaken, and destroy both the United States and Israel.

#### **D. Palestinian Islamic Jihad**

130. PIJ established itself in 1979 as a global, Sunni Islamist group dedicated to destroying Israel and creating an Islamic state in historic Palestine, including present-day Israel.

131. PIJ, like Hamas, viewed the United States and Israel as two inextricably connected enemies.

132. PIJ launched its first attacks on Israeli targets in Gaza in 1984, and, by the late 1980s, its leadership had been deported to Lebanon. PIJ deportees were later trained by the IRGC at camps operated by the terrorist group and IRGC proxy Hezbollah in Lebanon. PIJ, along with Hezbollah, has also conducted joint attacks on Israeli forces.

133. In 1992, PIJ established its formal operations arm: the Quds Brigades. Throughout the 1990s, PIJ carried out attacks in Israel to undermine the nascent Israeli-Palestinian peace process.

134. Since as late as 2018, PIJ has coordinated its attacks on Israel with Hamas and other military groups.

135. PIJ focuses primarily on violently confronting Israel through terrorist attacks, and it has regularly violated the laws of war when it committed its barbaric attacks.

136. Throughout PIJ's existence, the Islamic Republic of Iran—particularly the IRGC and its Qods Force—has supported, supplied, and trained PIJ terrorists.

137. PIJ was designated by the U.S. Secretary of State as an FTO in or about October 1997, and it has remained so-designated ever since. PIJ has been listed as an SDGT since 2001.

138. The Islamic Republic of Iran—particularly the IRGC and its Qods Force—has supported, supplied, and trained PIJ terrorists. Throughout that relationship, PIJ has played a significant role in Iran's regional and global campaign of supporting terrorism to further Iran's objectives, including damaging, weakening, and destroying both the United States and Israel.

**E. Al-Qaeda**

139. Osama bin Laden formed al-Qaeda in the late 1980s in Afghanistan in response to the Soviet occupation of Afghanistan. For decades, al-Qaeda has been a Sunni Islamic terrorist organization intent on destroying the United States.

140. Following the Soviet withdrawal from Afghanistan, Osama bin Laden began to transform al-Qaeda into a global terrorist group with the capability of launching attacks around the world. Bin Laden declared war on the United States in a published fatwa (religious decree) in 1996. In 1998, he declared a global jihad calling on all Muslims to kill Americans at any opportunity. On August 7, 1998, al-Qaeda suicide bombers in explosives-laden trucks attacked the U.S. embassies in Kenya and Tanzania, killing more than 200 people and wounding more than 5,000 others.

141. As a result of these and other terrorist attacks, the U.S. State Department designated al-Qaeda as an FTO on October 8, 1999. It remains designated as such to this day.

142. On September 11, 2001, al-Qaeda attacked the World Trade Center in New York and the Pentagon, killing thousands. A third attack, possibly aimed at the White House, was thwarted by passengers aboard United Flight 93.

143. In 2003, al-Qaeda turned its attention to sowing a campaign of terror in Iraq. Al-Qaeda believed that it could kill, injure, and terrorize Americans *en masse* there, and emphasized hostage-taking as a key tool. Al-Qaeda focused on indoctrination, propaganda, recruiting, and developing illicit networks necessary for smuggling fighters, money, and weapons into Iraq. On April 25, 2003, al-Qaeda issued a *fatwa* that declared jihad in Iraq and called on all pious Muslims to help attack and kill Americans there.

144. Al-Qaeda organized itself like a multinational corporation that had branches all over the world, but also partnered with affiliates.<sup>7</sup>

145. From the 2000s through 2010s, Al-Qaeda’s leadership in Afghanistan and Pakistan—which many dubbed “al-Qaeda Core”—cultivated a network of al-Qaeda branches in Afghanistan, Iraq, and Syria, among other places, who were often co-located with and/or used operatives simultaneously employed by al-Qaeda affiliates, like the Taliban. In Afghanistan and Pakistan, for example, Sirajuddin Haqqani simultaneously served as a member of al-Qaeda’s Military Council and Deputy Emir of the Taliban. Operations of the branches were led by al-Qaeda Core in Afghanistan and Pakistan, and were substantially financed and logistically supported by al-Qaeda’s cells in Western Europe.

146. To accommodate this organizational structure, al-Qaeda established, essentially, “parent/subsidiary” or “franchisor/franchisee” relationships between al-Qaeda Core (in Afghanistan and Pakistan) and branches like al-Qaeda-in-Iraq (“AQI”) (in Iraq and Syria). While al-Qaeda Core set the strategy, facilitated attacks and kidnapping, provided fighters and funding, and led the overall campaign, its branches—including AQI—conducted operations on a cellular level. Al-Qaeda thus operated in both a centralized and decentralized manner.

147. Al-Qaeda and its branches engaged in a continuous, two-way exchange of value. Al-Qaeda Core (in Afghanistan and Pakistan) supported al-Qaeda’s branches in Afghanistan,

---

<sup>7</sup> Al-Qaeda’s web of relationships are commonly described as “branches,” “franchises,” “affiliates,” “alliances,” and the like. As used in this Complaint, an al-Qaeda “branch” comprises another designated terrorist organization for which the leadership and members are formally part of al-Qaeda through, *inter alia*, their oath of loyalty to al-Qaeda and Osama bin Laden, and later, Ayman al-Zawahiri. An al-Qaeda “affiliate” comprises another designated terrorist organization for which the leaders and members have closely integrated with al-Qaeda to the point of being fused, but have not formally pledged an oath of allegiance. For example, al-Qaeda-in-Iraq was an al-Qaeda *branch*, while the Taliban was an al-Qaeda *affiliate*.

Iraq, and Syria—and the branches supported al-Qaeda Core. That two-way support took numerous forms, including financial support, training and sharing expertise in terrorist tradecraft, logistical support for terrorist operations, and managerial support. Al-Qaeda Core and its branches and affiliates used shared strategies, training sites, terrorist operatives, financiers, and the like, under the group’s multinational approach.

148. Al-Qaeda Core required every al-Qaeda branch, like AQI, to swear an oath of allegiance to al-Qaeda (which often swore a reciprocal oath to its counterpart), and al-Qaeda Core required its branches to follow al-Qaeda’s playbook concerning terrorist operations, finance, logistics, doctrine, and communication. Accordingly, all al-Qaeda members, including at its various branches, believed themselves—correctly—to be part of the same organization.

149. Al-Qaeda Core devised and oversaw AQI’s financial bureaucracy, which AQI operationalized and executed. The resulting financial infrastructure was purpose-built to ensure that the money both received was optimized to maximize the lethality of their terrorist campaign throughout Iraq, Syria, Afghanistan, and Pakistan. This infrastructure ensured that al-Qaeda Core and AQI senior leadership could redirect payments from one place to another.

150. The Islamic Republic of Iran—particularly the IRGC and its Qods Force—has supported, supplied, and trained al-Qaeda terrorists since the 1990s. Throughout, al-Qaeda has played a significant role in Iran’s regional and global campaign of supporting terrorism to further the IRGC’s goals, including damaging, weakening, and destroying the United States and Israel.

## **II. From 2014 Through 2024, ISIS Conducted Terrorist Attacks Targeting The United States**

151. The origins of ISIS trace to Abu Musab al-Zarqawi, a Jordanian terrorist who created a training camp in Afghanistan at Osama bin Laden’s invitation. By the time of the

September 11, 2001 terrorist attacks, Zarqawi had trained several thousand terrorists and established a terrorist network in Iraq, Syria, and other countries in the Middle East and Africa.

152. On or about October 15, 2004, the Secretary of State designated the Zarqawi terrorist network as an FTO under the name Jama'at al-Tawhid wa'al-Jihad. On or about the same day, the Secretary of State also designated Jama'at al-Tawhid wa'al-Jihad under Executive Order No. 13,224 as a SDGT.

153. In or around October 2004, Zarqawi formally pledged allegiance to al-Qaeda and renamed his terrorist network "al-Qaeda in Iraq." By then, Zarqawi and his organization were among the most prominent terrorists attacking Americans in Iraq and elsewhere.

154. A U.S. airstrike killed Zarqawi in June 2006. But AQI continued after his death as a formidable terrorist group waging a violent campaign against the United States. In 2010, a new AQI leader—Abu Bakr al-Baghdadi—took control of the AQI terrorist network.

155. In early 2011, shortly after Baghdadi's emergence, Syria spiraled into civil war. Many terrorist groups and other armed factions began vying for power, precipitating a near-total breakdown in Syrian governance and other civil institutions.

156. In 2013, reflecting AQI's expansion into Syria, Baghdadi changed AQI's name to the Islamic State of Iraq and Syria. On May 15, 2014, the Secretary of State again amended the AQI terrorist designation, this time to list the "Islamic State of Iraq and the Levant" as the organization's primary name (this is why U.S. government documents sometimes refer to the organization with the shorthand "ISIL"). On September 30, 2015 the Secretary of State amended that same designation to add more aliases: Islamic State, ISIL, and ISIS.

157. Unlike many militants fighting in Syria who aimed mainly to oppose the Syrian government, ISIS had a larger goal: the construction of a global terrorist caliphate. ISIS

attempted to control territory not through legitimate governance, but through widespread terror, criminality, and intimidation. Its acts of mass terrorist violence violated international law, including the laws of war.

158. ISIS committed acts of violence to intimidate civilians and cement its territorial control. According to the U.N. Human Rights Council in 2014, ISIS “made calculated use of public brutality and indoctrination to ensure the submission of communities under its control.” Its aim was “to subjugate civilians under its control and dominate every aspect of their lives through terror, indoctrination, and the provision of services to those who obey.” ISIS also publicly displayed the bodies of those it killed, and it executed hostages in public. It beheaded, shot, and stoned those it accused of crimes, notifying nearby residents before public executions were set to occur. ISIS particularly victimized women and children, whom it systematically abused and exploited.

159. ISIS targeted U.S. citizens to advance its terrorist objectives. After U.S. forces withdrew from Iraq in 2011, ISIS plotted attacks against U.S. persons and interests in Iraq and the region—including the brutal murder of kidnapped American citizens in Syria and threats to U.S. military personnel in Iraq. ISIS periodically released “kill lists” publicly broadcasting the names of hundreds of U.S. citizens whom it encouraged its operatives and followers to execute around the globe. It too often succeeded in murdering Americans.

160. ISIS ultimately seized control of wide swaths of territory, at its height controlling about 30% of Syria and 40% of Iraq. It was, in the words of Deputy Attorney General Lisa Monaco, “one of the most brutal terrorist organizations the world has ever known.”

### III. Defendants Knowingly Enabled Foreign Terrorist Organizations And Iran, The World's Foremost State Sponsor Of Anti-American Terrorism, To Conduct Hundreds Of Millions Of Dollars Of Prohibited Terrorist Finance Transactions

161. U.S. government reports have revealed that Binance and Zhao willfully enabled transactions by several terrorist organizations on the Binance exchange. Although the government reports do not provide granular details about each illicit transaction, it is extremely likely that a substantial percentage of these transactions involved *direct transfers of funds to terrorist organizations*. That is because terrorist organizations were notoriously using cryptocurrency as a tool to raise funds while evading sanctions, and so people and entities seeking to support those organizations used tools like Binance to effectuate those transfers.

162. Even transactions that were not direct one-way transfers of funds—*e.g.*, currency trades, where value went in both directions—helped FTOs by giving them access to the international financial system, which is otherwise blocked to them. What is more, Binance's practices allowed the terrorists to conduct transactions in secret, providing another layer of value to violent FTOs. And Binance affirmatively helped terrorists maintain that secrecy by refusing to file Suspicious Activity Reports about transactions that it knew involved terrorist accounts.

163. In the aggregate, these transfers enabled the IRGC, Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS to make, receive, and move *hundreds of millions* of U.S. dollars in violation of anti-terrorism sanctions designed to protect Americans from terrorist violence.

164. For example, FinCEN’s investigation discovered that Defendants knowingly allowed the following terrorist financing activities to occur on the Binance exchange between July 14, 2017, and July 30, 2023 (the “Relevant Period”):

- a. More than 200 direct bitcoin transactions, in the aggregate worth several hundred thousand dollars, with wallets associated with al-Qaeda.<sup>8</sup>
- b. Transactions involving two Syria-based money transmitters, primarily in 2019 and 2020, which had widely reported ties to terrorist financing, including ties to al-Qaeda campaigns.
- c. Multiple direct transactions between Binance and ISIS-associated wallets.
- d. Multiple transactions, each for thousands of dollars, with wallets used as fundraising tools for Hamas’s militant wing, the al-Qassam Brigades.
- e. Tens of millions of dollars in transactions with a network identified with the terrorist organization PIJ.
- f. Extensive suspicious activity involving BuyCash, a money transmitter that was added to OFAC’s SDN sanctions list in October 2023 for its involvement in Hamas fundraising, as well as ties to al-Qaeda and ISIS.
- g. Hundreds of thousands of direct trades between U.S. Binance.com users and Iranian Binance.com users—worth over a half billion dollars. These included transactions with sanctioned entities and individuals associated with the IRGC.

---

<sup>8</sup> “Wallets” in this context are software tools that users employ to access and trade virtual currencies. *See supra* “Cryptocurrency Primer.” Each wallet has an address that others can use to send currency to the wallet, and each wallet can be used to send currency to others. When users opened their accounts on Binance.com, Binance assigned them a wallet to conduct transactions.

165. OFAC found that Binance enabled systematic sanctions violations from August 2017 to October 2022, including at least 1,667,153 virtual currency transactions, totaling approximately \$706,068,127, that violated U.S. sanctions programs. These violations included 1,205,784 trades totaling \$599,515,938 in virtual currency and futures products between U.S. persons and Iranian counterparties; 42,609 trades totaling \$17,965,226 in transactions violating sanctions on Syria; and additional transactions between U.S. persons and counterparties in North Korea, and other sanctioned jurisdictions.

166. The Department of Justice found, and Binance admitted, that Binance “willfully caused transactions between U.S. users and users in comprehensively sanctioned jurisdictions in violation of U.S. law,” including “at least 1.1 million transactions” that violated sanctions prohibiting transactions between U.S. users and users residing in Iran, “with an aggregate transaction value of at least \$898,618,825.”

167. Defendants’ enabling of terrorist finance was willful. At all relevant times, Zhao and Binance’s management knew that Binance was subject to affirmative legal duties to block and report suspected terrorist finance and other illicit financial activity. Nevertheless, Zhao and Binance’s management not only refused to fulfill those duties, but instead deliberately circumvented them and enabled transactions by criminals and terrorist financiers.

168. Binance was required by law to establish an effective anti-money laundering (AML) program that was “reasonably designed to prevent” Binance “from being used to facilitate money laundering and the financing of terrorist activities.” 31 C.F.R. § 1022.210. Such programs include at least three key components: (1) “Know Your Customer” (KYC) policies designed to ensure that Binance did not provide services to prohibited or dangerous persons; (2)

transaction monitoring to block prohibited or dangerous transactions; and (3) reporting suspicious transactions to regulators, typically using Suspicious Activity Reports (SARs).

169. Binance flagrantly violated these obligations. For its first year of operation, Binance chose to employ no AML program at all. Binance then adopted an AML program that Binance knew had categorical gaps that rendered it ineffective against terrorist finance. Indeed, even when Binance's deliberately anemic AML program caught suspected terrorist finance activity, Binance's main focus was assisting its customers in continuing their transactions, and not preventing the prohibited activity.

170. With respect to KYC, Binance's procedures were designed to permit prohibited users to access its platform, and to keep Binance willfully blind to its prohibited users' characteristics. This was true both with respect to U.S. customers and to prohibited customers abroad, *e.g.*, sanctioned individuals and entities, and people in comprehensively sanctioned countries, including Iran.

171. Defendants were aware at all relevant times that because Binance served U.S. customers, it was subject to U.S. law, and that Binance was not compliant with U.S. law in many respects—including its intentional refusal to implement AML measures and its willful sanctions violations. But Binance wanted to have its cake and eat it too, *i.e.*, to keep its U.S. customers without complying with U.S. laws and regulations.

172. To accomplish that feat, Binance claimed, in 2019, that it would prevent all U.S. users from using Binance.com. Instead, Binance purported to route those users to a new U.S.-based cryptocurrency exchange called Binance.US, which would register with U.S. regulators and ostensibly comply with all relevant U.S. laws.

173. Behind the scenes, however, Binance was making efforts to retain its most valuable U.S. customers on Binance.com, shielded from oversight by U.S. regulators. When the Binance.US platform launched in 2019, Binance announced that it was implementing controls to block U.S. customers from the Binance.com platform. In reality, Binance did the opposite. Zhao directed Binance to assist high-value U.S. customers, referred to internally as “VIP” users, in circumventing those controls and to do so surreptitiously because—as Zhao himself acknowledged—Binance did not want to “be held accountable” for these actions. According to an SEC complaint, the Binance CCO explained, “[o]n the surface we cannot be seen to have US users[,] but in reality, we should get them through other creative means.” Indeed, Zhao’s stated “goal” was “to reduce the losses to ourselves, and at the same time to make the U.S. regulatory authorities not trouble us.”

174. On a June 25, 2019 call, Binance employees and executives told Zhao that they were implementing the plan by contacting U.S. VIP users “offline,” through direct phone calls, “leav[ing] no trace.” If a U.S. VIP user owned or controlled an offshore entity outside of the United States, Binance’s VIP team would help the VIP user register a new, separate account for the offshore entity and transfer the user’s VIP benefits to that account, while the user transferred its holdings to the new account. On the same call, an employee described a script that Binance employees could use in communications with U.S. VIPs to encourage them to provide non-U.S. KYC information to Binance by falsely suggesting that the user was “misidentified” in Binance’s records as a U.S. customer. Zhao authorized and directed this strategy, explaining on the call, “[w]e cannot say they are U.S. users and we want to help them. We say we mis-categorized them as U.S. users, but actually they are not.”

175. Also during the call on or around June 25, 2019, a senior employee provided guidance on what Binance should not do: “We cannot advise our users to change their KYC. That’s, that’s of course against the law.” The senior employee provided an alternative route to the same end: “But what we can tell them is through our internal monitoring, we realize that your account exhibits qualities which makes us believe it is a US account ... if you think we made a wrong judgment, please do the following, you know, and we have a dedicated customer service VIP service officer.” The senior employee described Binance’s plan as “international circumvention of KYC.”

176. In 2020, internal conversations at Binance revealed that it was using Binance.US as a laboratory to see which customers would trade high volumes, and then covertly migrating those customers to Binance.com. Thus, Binance employees agreed that users would first “onboard with US, then if their volume is really big we will push hard on .com to accept it on an exceptional basis . . . CZ [Zhao] will definitely agree to this” because “we always have a way for whales”—lucrative high-volume users—to access Binance.com.

177. Binance, at Zhao’s direction, agreed to and implemented this strategy to keep U.S. VIP users on Binance.com as documented in an internal document titled “VIP handling.”

178. Separately, prior to August 2021, Binance allowed users to open “Level 1” or “Tier 1” accounts *without submitting any KYC information*. Instead, users could open Level 1 accounts simply by providing an email address and a password. Binance required no other information, including the user’s name, citizenship, or location. A Level 1 account holder could deposit virtual currency into its account and then transact in an unlimited amount of virtual currency. While Level 1 accounts had certain limitations, including a virtual currency withdrawal limit of up to the value of two Bitcoins per day, Binance allowed users to open multiple Level 1

accounts by providing a new email address for each account, which effectively circumvented the withdrawal limit. Even if a user adhered to the daily two Bitcoin withdrawal limit on a single account, for most of Binance’s existence, the user could still withdraw thousands-and sometimes many tens of thousands of U.S. dollars due to the rising value of a single Bitcoin, which increased from approximately \$3,000 to \$63,000 in value between December 2018 and April 2021. Level 1 accounts comprised the vast majority of user accounts on Binance.com.

179. Binance also circumvented its own limitations on Level 1 accounts. For example, in a July 17, 2020 chat, senior Binance employees explained that “for our biggest traders/VIPs,” we “can bypass [limitations on non-KYC accounts, such as withdrawal limits],” but clarified that this was “SPECIAL treatment” reserved only for preferred customers.

180. In August 2021, Binance announced that it would require all new users to submit full KYC information. But Binance allowed existing users who had not submitted KYC information—including all Level 1 accounts (which were the majority of Binance’s user accounts)—to trade on the platform without providing full KYC information until May 2022.

181. As a result, U.S. users (including those supporting terrorist groups) were able to continue opening accounts on Binance.com without providing any KYC information that would identify them as U.S. users.

182. Because *Binance effectively had no KYC information about the majority of its customers*, it represented that it would block prohibited users from accessing Binance.com by blocking users who attempted to access the platform using an Internet Protocol (IP) address corresponding to a U.S. location. But Binance openly guided users to use Virtual Private Networks (VPNs), which are free, simple software that can mask a user’s IP address, as a means to circumvent this barrier. Indeed, as early as April 2019, Binance posted a guide on its own

website entitled “A Beginner’s Guide to VPNs,” which explained to customers that they could conceal their locations using VPNs—even going so far as to say “you might want to use a VPN to unlock sites that are restricted in your country.” The CFTC uncovered transcripts of internal chat conversations, held in 2019 and onwards, where Zhao and other senior executives confirmed that covertly advising customers to use VPNs to circumvent Binance’s own IP address blocks was a high-level business decision.

183. Binance’s efforts to covertly keep its U.S. customers on Binance.com succeeded. As of January 2020, approximately 19.9 percent of Binance’s customers were located in the United States. As of June 2020, approximately 17.8 percent of Binance’s customers were still located in the United States. This was even though Binance ostensibly blocked all U.S. customers starting in 2019.

184. Binance’s efforts to conceal its U.S. user base served a single purpose: avoiding scrutiny by U.S. regulators. Binance and Zhao feared such scrutiny because they knew that Binance.com was blatantly violating U.S. law, including anti-terrorism sanctions. Thus, in 2018, Binance’s Chief Compliance Officer wrote to Zhao that users from sanctioned countries were on Binance.com, and asked whether their IP addresses should be blocked. No block occurred at that time, and in any event, Binance knew that an IP-address block could be circumvented using VPNs (as it encouraged its users to do). Later, in 2019, Zhao himself explained to another senior leader that “The United States has a bunch of laws to prevent you and Americans from any transaction with any terrorist,” adding that “you only need to serve Americans or service U.S. sanctioned country” to be implicated. Zhao and Binance deliberately evaded those laws, which were (and are) an important part of the United States’ efforts to interdict terrorist financing and prevent terrorist attacks.

185. The flip side to Binance’s actions to conceal its U.S. customer base was Binance’s actions vis-à-vis prohibited users abroad, including criminals, terrorist financiers, and individuals and entities who were either on sanctions lists or residing in comprehensively sanctioned countries. Binance ostensibly sought to prevent those prohibited users from accessing Binance.com—but those measures were shams: Binance made them intentionally weak to begin with, and then circumvented them even further to allow prohibited persons to use the platform.

186. As with U.S. users, *international users—such as those in Iran and members of foreign terrorist organizations—likewise were not subject to KYC requirements to open Level 1 accounts prior to August 2021*. And as with U.S. users, international users could circumvent IP-address blocks (which were used to block access from comprehensively sanctioned countries) using VPNs. Any minimally savvy user who did not commit those basic errors could open and use a Binance.com account, trading and receiving currency through Binance. In effect, then, Binance remained open to prohibited users.

187. Binance knew this. Repeated internal conversations stressed that without KYC information it was impossible to effectively prevent users in sanctioned jurisdictions from accessing the platform.

188. To the extent Binance did implement any controls, those controls were paper thin. Binance frequently chose not to close the prohibited accounts that it knew about, and blocked users could contact customer support and successfully ask Binance to reactivate their account. This problem was pervasive. The government found, for example, that Binance continued to serve *thousands* of users that employees had identified as being from comprehensively sanctioned countries—including, for example, more than 7,000 accounts that had submitted KYC documents from a comprehensively sanctioned country and more than 12,500 users who

had provided Iranian phone numbers. This was even though Binance's official stance was that it had blocked all Iranian customers. Indeed, a year after Binance claimed to have blocked all Iranian accounts, it found approximately 600 "verified level 2" users from Iran, *i.e.*, users who had gone through Binance's KYC process but remained on the platform.

189. As an additional way to avoid conducting KYC, Binance deliberately enabled large entity customers, including exchange brokers, to directly access Binance.com through sub-accounts created by the broker under its own account. Binance knowingly enabled exchange brokers to create up to 1000 sub-accounts under their master accounts, and did not subject those sub-account users to any meaningful scrutiny. This allowed multiple exchange brokers that had been designated by OFAC (and those brokers' users) to access Binance.com and conduct hundreds of millions of dollars in suspicious transactions.

190. Binance's AML deficiencies went far beyond poor KYC. Binance also refused to implement proper transaction monitoring, and refused to report suspicious activity. Indeed, Binance ***did not file a single SAR*** describing the suspicious conduct in the United States as of May 2022—despite the fact that almost all of the transactions described in this complaint had occurred prior to that date. Instead, Binance allowed millions of suspicious transactions to proceed without disclosing any of them to regulators.

191. Binance lied about the state of its compliance program both to U.S. regulators and to partner businesses. Thus, in August 2019, Binance's Chief Compliance Officer falsely assured a U.S. state regulator that Binance "provides for AML/CFT controls to ensure the safe and legitimate use of our platforms," "screens all its customers prior to the establishment of a business relations or undertaking a transaction against OFAC, EU, UK and Hong Kong sanctions," and performs "customer due diligence," including where "there is suspicion of

money laundering or terrorism financing.” All of that was false at the time, and remained false. In fact, as of December 2019, that same Chief Compliance Officer admitted in a message to a colleague that Binance.com “doesn’t even do AML namescreening/sanctions screening.”

192. Similarly, when a business partner requested a compliance audit, Binance “purposely engaged a compliance auditor that would ‘just do a half assed individual sub audit’” to “‘buy us more time.’” Binance’s Money Laundering Reporting Officer lamented that she “need[ed] to write a fake annual MLRO report,” and the Chief Compliance Officer assured her “yea its fine I can get mgmt.. to sign” off on the fake report.

193. Binance also enabled obfuscation by processing transactions for entities known as cryptocurrency mixers, which are entities that attempt to thwart the transparency of the blockchain by scrambling transactions together to obscure flows of funds. Mixers are an essential tool for money launderers, whose mission is to hide the sources and destination of ill-gotten money. Binance processed tremendous volumes for mixers. OFAC, for example, found that Binance processed more than \$275 million in deposits and more than \$273 million in withdrawals from February 2018 to May 2019 for BestMixer, a prominent entity in the space, which was shut down by Dutch authorities in May 2019.

194. Binance also listed six of the highest-trading anonymity-enhanced cryptocurrencies (AECs) for trading on Binance.com. These cryptocurrencies use advanced programming to obscure transaction details. For example, the most popular one, Monero, inserts false information into every channel on its private blockchain, which effectively conceals sender data and hides transaction amounts. This coin is designed to make supervisory transaction monitoring virtually impossible. As FinCEN explained, these coins “pose heightened money

laundering and terrorist finance risks.” Binance offered trading in these coins with essentially no oversight.

195. Binance’s willful misconduct directly led, according to FinCEN, “to the platform being used to process transactions related to . . . unregistered convertible virtual currency mixing services uses to launder illicit proceeds, high-risk jurisdictions, individuals listed on OFAC’s SDN List, [and] terrorist financing.” FinCEN determined that Binance’s willful refusal to report hundreds of thousands of suspicious transactions “inhibited law enforcement’s ability to disrupt the illicit actors” and that its conduct “extensively harmed FinCEN’s mission to safeguard our financial system from illicit use” and “expos[ed] the U.S. financial system to a significant volume of illicit financial activity.”

196. Defendants’ conduct shows that their representations that Binance would block prohibited users were false when made. Instead of accurately representing Defendants’ views, these false statements served only to deceive regulators and others concerned about Binance’s misconduct.

197. FinCEN’s review of Binance’s transactions was extensive but not comprehensive. As stated in its settlement agreement, it had identified “hundreds of thousands of potentially suspicious transactions that went through the Binance platform.” But, as part of its settlement with FinCEN, Binance must engage a consultant to perform a SAR lookback review of its transactions between January 1, 2018 and December 31, 2022 and to report on the findings no later than May 2025, to be followed by the filing of any necessary SARs within 90 days of the report. Further review will identify substantial additional transactions that funded designated FTOs. Indeed, OFAC identified more than \$600 million worth of transactions between U.S. persons and crypto wallets known to be located in or otherwise connected with Iran, the world’s

foremost state sponsor of anti-American terrorism, and tens of millions of dollars of additional transactions between U.S. persons and crypto wallets located in or otherwise connected with Syria, another funding source. This misconduct allowed at least millions of dollars to flow to the FTOs that committed the attacks that injured Plaintiffs.

198. More broadly, the foregoing includes only some of the most salient facts about Binance's AML and sanctions-compliance violations. As the government found (and as Defendants admitted), the company knew that it was required to implement an AML program and to comply with U.S. sanctions, deliberately refused to do so, obscured that fact through various deceptive means, and repeatedly and flagrantly violated those laws. The examples provided *supra* illuminate this pervasive and systemic pattern of illegal activity. Discovery will show substantially more violations occurring contemporaneously with the attacks in this case, causing even more value to flow through to the FTOs who committed the attacks.

#### **IV. Defendants Were Generally Aware That The Terrorist Attacks On Plaintiffs And Their Family Members Were A Foreseeable Consequence Of Willingly Enabling Foreign Terrorist Organizations' Transactions On The Binance Exchange**

199. The terrorist attacks that injured Plaintiffs were a foreseeable consequence of Defendants' unlawful assistance to FTOs. Multiple warnings—from the U.S. government, international authorities including the United Nations, blockchain analysts, and terrorism scholars—made it clear to the entire financial sector that enabling the specific terrorist organizations that attacked Plaintiffs to conduct international financial transactions of the types that Binance enabled would lead to terrorist attacks on Americans. These warnings, individually and collectively, establish that the attacks in this case were a foreseeable consequence of Defendants' unlawful conduct, and that Defendants were at least generally aware of their role in the FTOs' unlawful activities, including terrorist finance and terrorist violence.

**A. Defendants Were Generally Aware that FTOs Embraced Cryptocurrency to Fund Terrorist Attacks**

200. Both prior to Binance’s founding and throughout the events described in this Complaint, Defendants were generally aware that cryptocurrency posed uniquely dangerous terrorist financing risks. A steady drumbeat of official warnings came from the U.S. government, the United Nations, the Financial Action Task Force, and other members of the international community. Beyond that, there was abundant reporting in both the mainstream media and media focused on cryptocurrency and digital assets (*i.e.*, “cryptopress”). Further still, blockchain analysis firms, cryptocurrency and terrorist-finance scholars, and NGOs similarly sounded the alarm that terrorist groups were actively looking to use—and did in fact use—cryptocurrency to fund their operations and commit attacks.

201. Binance knew about these warnings. As a global cryptocurrency exchange, Binance regularly monitored (but willfully disregarded) warnings from the U.S. government, international community, and blockchain analysis firms about the risks of illicit use of cryptocurrency by FTOs, including by monitoring reporting in mainstream media and the cryptopress. Binance was also told directly about these warnings by the blockchain analysis firms whose AML/CFT/KYC monitoring services Binance contracted for and used. *See infra* Part V(C).

202. Zhao, similarly, knew about these warnings. As the CEO of a global cryptocurrency exchange and a highly active member of the cryptocurrency community, Zhao regularly monitored (but willfully disregarded) warnings from the U.S. government, international community, and blockchain analysis firms about the risks of illicit use of cryptocurrency by FTOs, including by monitoring reporting in mainstream media and the cryptopress. Zhao’s active accounts on social-media platforms such as Twitter and Reddit, for example, demonstrated that

he kept current on major developments in the cryptocurrency industry, such as the warnings and news discussed below. On information and belief, Zhao was also told directly about these warnings by the blockchain analysis firms whose AML/KYC monitoring services Binance contracted for and used. *See infra* Part V(C).

### **1. Warnings from the U.S. Government**

203. U.S. government agencies and high-ranking officials issued dozens of warnings to financial institutions and other actors in the cryptocurrency space—including cryptocurrency exchanges, like Binance—that cryptocurrency posed terrorist financing risks. These warnings emphasized that many of the features that could make cryptocurrency adoption attractive to everyday people, such as the speed and low cost of cross-border transactions and the medium’s relative pseudonymity, were extremely attractive to terrorists and other bad actors. Not only did the U.S. government itself publicize these warnings, but those warnings also regularly received substantial coverage in mainstream media outlets and the cryptopress. Each warning—and certainly the warnings in aggregate—gave Defendants general awareness of the terrorist-financing risks posed by cryptocurrency.

204. The following warnings from U.S. government agencies and high-ranking officials are illustrative of the type of warnings issued before and during the Relevant Period.

205. As early as 2008, DOJ recognized the risk that “[d]igital currencies . . . are vulnerable to money laundering and terrorist financing.” In 2013, the Director of FinCEN testified before Congress that the bureau was aware that “virtual currency . . . is being used to transact payments” and “has been exploited by some pretty serious criminal organizations.” Accordingly, FinCEN committed to focus on “protect[ing] the U.S. financial system . . . from those illicit actors . . . laundering or moving money for the purposes of terrorism.” The U.S. government’s warnings grew only more detailed and urgent over time.

206. In February 2018, Treasury Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker highlighted in a speech before industry that Treasury has “seen terrorist groups . . . use digital and virtual currencies to hide their ill-gotten gains and finance their illicit activities.”

207. In November 2018, Treasury issued its *Agency Financial Report, Fiscal Year 2018*, where the department explained that it was combating terrorism by FTOs “the Islamic State of Iraq and Syria (ISIS), al-Qaida, Hizballah, Hamas, the Taliban and others” by using its role as FATF President to “clarif[y] how the FATF standards apply to virtual asset service providers, which include virtual currency exchangers and administrators and how countries under the FATF standards must license or register and regulate them for AML/CFT, and monitor them for compliance with their AML/CFT obligations.”

208. In July 2019, Treasury Secretary Steven Mnuchin gave a detailed speech about regulatory issues associated with cryptocurrency. During that widely publicized speech, Secretary Mnuchin warned of the “***serious concerns*** that Treasury has regarding the growing misuse of virtual currencies by money launderers, ***terrorist financiers***, and other bad players.” (Emphasis added.) Highlighting it as “a national security issue,” Sec. Mnuchin warned that “[c]ryptocurrencies, such as Bitcoin, have been exploited to support billions of dollars of illicit activity.”

209. In October 2020, the DOJ published the *Report of the Attorney General’s Cyber Digital Task Force: Cryptocurrency Enforcement Framework*, which, among other things, included detailed warnings about the various ways that terrorist groups continued to embrace cryptocurrency. As DOJ explained, it had recently seized “hundreds of thousands of dollars’ worth of bitcoin” by “dismantling . . . terrorist financing campaigns . . . involving Hamas’s

military wing, al-Qaeda, and ISIS.” According to DOJ, there were several ways in which terrorist groups had already embraced cryptocurrency. Per DOJ, one was fundraising: “it is clear that terrorist networks have conducted fundraising operations through Internet-based crowdsource platforms in an attempt to evade stopgaps built into the international banking system,” like when an ISIS supporter “us[ed] social media to instruct donors on how bitcoin could provide untraceable financial support” in 2015, and efforts by “the al-Qassam Brigades (Hamas’s military wing), al-Qaeda, and ISIS” to use “cryptocurrency technology and social media platforms to spread their influence and raise funds for terror campaigns.” These “terrorist groups have solicited cryptocurrency donations running into the millions of dollars via online social media campaigns.”

210. Moreover, according to that same October 2020 DOJ report, “terrorists also use cryptocurrency to buy and sell ‘tools of the trade’—*i.e.*, items that may or may not themselves be unlawful but are used for subsequent unlawful conduct. Such tools include raw materials to manufacture drugs or explosives, as well as cyber tools and computing capabilities (including servers and domains) to engage in cybercrime or to conduct malign influence campaigns over social media.” Terrorists could also transfer cryptocurrency “often in large amounts” “across international borders.” Cryptocurrency thus offered terrorist groups “a tool to circumvent traditional financial institutions in order to obtain, transfer, and use funds to advance their missions.” DOJ concluded its report by warning that “[c]urrent terrorist use of cryptocurrency may represent the first raindrops of an oncoming storm of expanded use that could challenge the ability of the United States and its allies to disrupt financial resources that would enable terrorist organizations to more successfully execute their deadly missions”; accordingly, terrorist “uses of cryptocurrency threaten not just public safety, but national security.”

211. In February 2021, Treasury Secretary Janet Yellen commented during a public roundtable that the “misuse of cryptocurrencies and virtual assets is a growing problem,” including because “cryptocurrencies have been used” as “a tool to finance terrorism.”

212. During a July 2021 congressional hearing, U.S. Representative Elissa Slotkin explained that “new tech like cryptocurrencies, which are decentralized, largely anonymous forms of digital money, have enabled terrorists to further expand and disguise their funding efforts.” During that same hearing, a high-ranking official in the Department of Homeland Security commented on the “increasing use of cryptocurrency, particularly regarding soliciting donations and fundraising,” so “as the technology becomes more accessible and easier for the user, it is going to be more common among terrorist groups.” And another high-ranking official in the Department of Homeland Security commented that “terrorist organizations . . . have grown increasingly more technical in their approach to obfuscating their criminal acts, while also morphing operations to the perceived anonymity of the darknet. . . . [C]ryptocurrency can now be used with relative ease to facilitate any type of illicit activity.” He observed there had been a “marked increase” in cryptocurrency seizures that year, “signif[ying] growing confidence in cryptocurrency use by bad actors.”

213. In or around June 2023, Treasury Under Secretary for Terrorism and Financial Intelligence Brian Nelson publicly explained that “[a]s virtual assets continue to become more accessible and barriers to entering the crypto market continue to decrease, we need to be mindful of the potential for illicit financial activity . . . . [W]e know that terrorist groups try to exploit emerging technologies for their organizations; this has been true for a long time. And we have seen both domestic and foreign terrorist actors utilize virtual assets to fund their operations.”

214. Defendants were generally aware of these U.S. government warnings, each of which independently conveyed to Defendants that terrorist organizations may seek to transact using cryptocurrency on its exchange and that these terrorist organizations used cryptocurrency to fund their operations and commit terrorist attacks. Despite this general awareness, Defendants willfully disregarded AML/CFT requirements and enabled terrorist groups to transact on the Binance.com exchange.

## 2. Warnings from the International Community

215. Members of the international community also repeatedly warned about the possibility—and reality—of terrorist use of cryptocurrency. Each warning, and certainly the warnings in aggregate, gave Defendants general awareness of the terrorist-financing risks posed by cryptocurrency. The following are illustrative examples of warnings issued during the Relevant Period.

216. **The United Nations.** The U.N., both through Resolutions and proclamations from Member States during high-level, public summits, warned that cryptocurrencies risked funding FTO attacks. In 2019, for example, U.S. Security Council Resolution 2462 (2019) highlighted the U.N.’s “grave concern” that: (1) “terrorist groups may move and transfer funds . . . through the use of emerging payment methods, such as . . . virtual-assets”; and (2) regardless of the merits of “innovations in financial technologies,” they “present a risk of being misused, including for terrorist financing.” In connection with the Resolution, Member State representatives warned that “[t]errorist groups are increasingly making use of cryptocurrency.”

217. Beyond that, U.N. reports in 2021 warned about “several notable instances” including “in the 2019 Sri Lankan bombings” where the “number of transactions in Bitcoin wallets used by ISIL to raise funds increased notably before the bombings, leading to the belief that these Bitcoins played a role in financing the attacks.”

218. **Financial Action Task Force.** FATF was—and remains—the global standard setting body for AML/CFT. FATF regularly warned that cryptocurrencies risked funding FTO attacks. In 2018, for example, FATF warned that “[v]irtual currencies/crypto-assets facilitate easy online access and global reach which make them attractive to move and store funds for money laundering and terrorist financing.”

219. FATF reiterated those warnings throughout the Relevant Period. In September 2020, for example, FATF explained that the “distinct features” of cryptocurrencies “create new opportunities for . . . terrorist financiers,” highlighting the “ability to transact across borders rapidly.” FATF even published reports targeted at virtual assets service providers, like Binance, regarding “money laundering” and “terrorist financing” “red flag indicators.”

220. Defendants knew about FATF and its warnings regarding terrorist use of cryptocurrencies. Binance touted FATF and its role in AML/KYC standard-setting in Binance’s “Binance Academy” resource on its website. Binance employees, including Binance’s former Chief Compliance Officer, similarly knew that “FATF’s recommendations function as a global standard in which the industry is trying to band together to achieve.’ And FATF itself hosted “private sector consultative forum[s] on the various services and business models in the digital currency space,” that addressed “how industry can comply with vital AML/CFT obligations.”

221. Defendants were generally aware of these warnings from the international community—including, but not limited to, warnings from the United Nations and FATF—each of which independently conveyed to Defendants that terrorist organizations may seek to transact using cryptocurrency on its exchange and that these terrorist organizations used cryptocurrency to fund their operations and commit terrorist attacks. Despite this general awareness, Defendants

willfully disregarded AML/CFT requirements and enabled terrorist groups to transact on the Binance.com exchange.

### **3. Warnings from Blockchain Analysis Firms, Terrorism Scholars, and NGOs**

222. Blockchain analysis firms, moreover, regularly warned that cryptocurrencies risked funding attacks by FTOs.

223. In 2020, for example, blockchain analytics firm Elliptic warned of terrorist use of cryptocurrency when it publicly reported about the “the dismantling of three crypto-based terrorist financing campaigns associated with al-Qassam Brigades, Hamas’s military wing, al-Qaida and the Islamic State of Iraq and the Levant (ISIS)” by DOJ.

224. In January 2020, likewise, Chainalysis, a leading blockchain analytics firm—and one of Binance’s own compliance vendors—published a report warning that “from the investigations [it had] been involved with in 2019 that there’s some cause for concern. What’s especially worrying are the advancements in technical sophistication that have enabled successful terrorism financing campaigns using cryptocurrency.” Looking ahead, Chainalysis cautioned that it was “possible that in 2020 and beyond, more terrorist organizations will embrace cryptocurrency as a fundraising tool and push for further advancements that allow them to take in more funds and enhance their privacy. Terrorist groups have proven adept at leveraging emerging technologies to advance their agenda.” Thus, Chainalysis urged, “the cryptocurrency community as a whole must remain vigilant to ensure this doesn’t happen.” In 2021, Chainalysis’s Global Head of Policy and Regulatory Affairs testified before Congress that “[t]hrough blockchain analysis,” Chainalysis confirmed that “terrorist organizations . . . have used cryptocurrency in an attempt to weaken the impact or fully circumvent sanctions.”

225. In February 2021, similarly, blockchain analytics firm CipherTrace warned that “[t]errorist organizations and their supporters and sympathizers are continuously looking for new ways to raise and transfer funds without detection or tracking by law enforcement. An asset like cryptocurrency, which allows for the instant, pseudonymized transmission of value around the world with no due diligence or recordkeeping, was bound to catch their eye.”

226. Defendants were generally aware of these warnings from blockchain analysis firms, each of which independently conveyed to Defendants that terrorist organizations may seek to transact using cryptocurrency on the Binance exchange and that these terrorist organizations used cryptocurrency to fund their operations and commit terrorist attacks. Despite this general awareness, Defendants willfully disregarded AML/CFT requirements and knowingly enabled terrorist groups to transact on the Binance.com exchange.

227. **Terrorism scholars and NGOs** also publicly warned that cryptocurrencies risked funding attacks by FTOs. In 2016, for example, Brigitte Nacos warned that terrorists were using cryptocurrencies as ways of “Raising Funds to Finance Their Operations”—*i.e.*, terrorist attacks:

[T]ransnational [terrorist] groups have used their websites to raise funds to finance their operations [i.e., terrorist attacks]. ... Nobody, however, is as sophisticated as jihadists and their supporters who are known to have discussed in various social media the advantages of Bitcoin as ideal currency for raising donations and purchasing weaponry.

**B. Defendants Were Generally Aware That The IRGC, Hezbollah, and Kataib Hezbollah Embraced Cryptocurrency to Fund Terrorist Attacks**

228. Both prior to Binance’s founding and throughout the events described in this Complaint, Defendants were generally aware that the IRGC sought to exploit cryptocurrency and cryptocurrency exchanges, like Binance, to sustain their campaign of terrorist attacks, including by supporting their proxies’ terrorist attacks.

229. Before and throughout the Relevant Period, warnings of the IRGC’s embrace of cryptocurrency were legion and came from all sorts of bodies—including the U.S. government, blockchain analysis firms, terrorism scholars, and NGOs.

230. The IRGC itself loudly proclaimed its embrace of cryptocurrency. Indeed, as reported in the cryptopress, in or around early 2020, “Saeed Muhammad, commander of [IRGC] said in a speech . . . that Iran should look to cryptocurrencies to bolster international investment despite heavy sanctions on the nation.” The IRGC thus “demand[ed] the creation of a more sophisticated mechanism (a commodities exchange) to bypass sanctions,” and facilitate “the exchange of products and the use of cryptocurrencies with [its] partnerships” with other countries.

231. Binance knew about these warnings. As a global cryptocurrency exchange, Binance regularly monitored (but willfully disregarded) warnings from the U.S. government, U.N., and blockchain analysis firms about the risks of illicit use of cryptocurrency by Iran and the IRGC, including by monitoring reporting in mainstream media and the cryptopress. Binance was also told directly about these warnings by the blockchain analysis firms whose AML/KYC monitoring services Binance contracted for and used. *See infra* Part V(C).

232. Zhao, similarly, knew about these warnings. As the CEO of a global cryptocurrency exchange and a highly active member of the cryptocurrency community, Zhao regularly monitored (but willfully disregarded) warnings from the U.S. government, international community, and blockchain analysis firms about the risks of illicit use of cryptocurrency by Iran and the IRGC, including by monitoring reporting in mainstream media and the cryptopress. Zhao’s active accounts on social-media platforms such as Twitter and Reddit, for example, demonstrated that he kept current on major developments in the cryptocurrency industry, such as

the warnings and news discussed below. On information and belief, Zhao was also told directly about these warnings by the blockchain analysis firms with which Binance had contractual relationships related to those firms' AML/KYC monitoring. *See infra* Part V(C).

### 1. Warnings from the U.S. Government

233. The U.S. government issued warnings—including directly to cryptocurrency exchanges, like Binance—that alerted Defendants that the IRGC embraced cryptocurrency to evade U.S. sanctions and fund attacks.

234. In October 2018, FinCEN issued a detailed *Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System*. That Advisory was targeted to financial institutions, including virtual currency exchanges like Binance. FinCEN warned that in Iran “virtual currency is an emerging payment system that may provide potential avenues for individuals and entities to evade sanctions.” Iranians could “access virtual currency platforms” through “Iran-located, Internet-based virtual currency exchanges” as well as “U.S.- or other third country-based virtual currency exchanges.” FinCEN thus warned that “[i]nstitutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran,” and they should “have the appropriate systems to comply with all relevant sanctions requirements and AML/CFT obligations.” And FinCEN underscored that “a non-U.S.-based exchanger or virtual currency provider doing substantial business in the United States is subject to AML/CFT obligations and OFAC jurisdiction.”

235. In that same 2018 FinCEN advisory, the bureau warned: “The Iranian regime has long used front and shell companies to exploit financial systems around the world to generate revenues and transfer funds in support of malign conduct, which includes support to terrorist groups [and] ballistic missile development.” FinCEN also “highlight[ed] the Iranian regime’s exploitation of financial institutions worldwide, and describe[d] a number of typologies used by

the regime to illicitly access the international financial system and obscure and further its malign activity. It also provide[d] red flags that may assist financial institutions in identifying these methods.” Critically, FinCEN explicitly connected Iran’s embrace of cryptocurrencies to its support for the IRGC and its terrorist proxies: Iran “may seek to use virtual currencies” “to fund the regime’s nefarious activities, including providing funds to the Islamic Revolutionary Guard Corps (IRGC) and its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), as well to Lebanese Hizballah, Hamas, and other terrorist groups.” FinCEN’s warning about Iran’s embrace of cryptocurrency to fund terrorism was widely publicized, including by the cryptopress and blockchain analysis firms whose reporting Defendants closely monitored.

236. In November 2019, in connection with Iran being designated as a jurisdiction of primary money laundering concern, Treasury reiterated FinCEN’s earlier warning that Iran may “seek to exploit virtual currencies” to “fund the Islamic Revolutionary Guard Corps (IRGC), its Islamic Revolutionary Guard Corps Qods Force (IRGC-QF), Lebanese Hizballah (Hizballah), Hamas, the Taliban and other terrorist groups.”

237. In October 2020, DOJ warned that “Iran . . . may turn to cryptocurrency to fund cyber-attacks, blunt the impact of U.S. and international sanctions, and decrease America’s influence in the global marketplace.” Accordingly, “cryptocurrency exchanges—including those physically located outside the United States—must take seriously their legal and regulatory obligations, discussed in greater detail below, to protect users and to safeguard potential evidence in criminal or national security investigations.”

238. Defendants were generally aware of these warnings from the U.S. government, each of which independently conveyed to Defendants that actors in the Government of Iran and the IRGC may seek to transact using cryptocurrency on its exchange and that they used

cryptocurrency to fund their operations and commit terrorist attacks. Despite this general awareness, Defendants willfully disregarded AML/CFT requirements and enabled the IRGC and its affiliates to transact on the Binance.com exchange.

## **2. Warnings from Blockchain Analysis Firms**

239. Defendants were also made generally aware of Iran's and the IRGC's embrace of cryptocurrency through public warnings issued by blockchain analysis firms, including several firms that had contractual relationship with Binance.

240. In May 2021, for example, leading blockchain analysis firm CipherTrace warned that a "trend detected by CipherTrace analysis is the substantial use of cryptocurrency in sanction[ed] geographies--most notably, Iran. As [OFAC] ramps up its enforcement actions against virtual asset service providers for sanctions violations related to blocked countries, it is vital that institutions screen IP data to ensure they aren't transacting with sanctioned entities and addresses. CipherTrace detected more than 72,000 unique IP addresses linked to Iran. These addresses were either involved in direct cryptocurrency transactions or were used to query the blockchain to verify funds in cryptocurrency addresses that they control." CipherTrace also warned that "if financial institutions, including exchanges, facilitate payments for an individual or company in Iran, those institutions would be exporting services to that person or entity in violation of the Iranian Transactions Regulations."

241. In June 2021, similarly, Chainalysis's Global Head of Policy and Regulatory Affairs issued a detailed warning and explanation of Iran's comprehensive effort to embrace cryptocurrencies to evade sanctions during testimony before Congress:

Iranian officials have discussed the use of cryptocurrencies to evade sanctions, with Iranian researchers preparing whitepapers on the topic. The Central Bank of Iran has piloted research and development of a Central Bank Digital Currency (CBDC). Recently, Iranian President Hassan Rouhani requested his government start developing a framework to regulate cryptocurrencies. Beyond the

government level, Iran's citizens have embraced cryptocurrency and are considered early adopters. The two main ways Iran can use cryptocurrency to evade sanctions, or weaken the impact of sanctions, is to acquire wealth by mining or theft of cryptocurrencies, or to use cryptocurrencies to conduct economic business to bypass traditional screening. ***Iran is heavily involved in mining cryptocurrencies.*** By mining cryptocurrencies, Iran is able to acquire wealth by validating cryptocurrency payments for individuals globally - including U.S. citizens. They can then transact via non-traditional financial institutions, including high risk exchanges or individual peer-to-peer traders, to ***bypass screening.*** Iran's cyber actors have been involved with ***deploying ransomware and receiving cryptocurrency payments*** from U.S. companies. While there has not been substantial reporting on exact use cases for economic trades involving cryptocurrency, Iran could use cryptocurrency to ***send and receive payments for oil or other goods to evade sanctions.*** According to a report from the English-language Iranian economic news source Financial Tribune, the Central Bank of Iran is authorizing banks and licensed exchanges to use cryptocurrency as payments for imports. Chainalysis research has identified over 20 Iranian exchanges that have received cryptocurrencies worth ***over \$820 million*** since May 2013. Substantial amounts of the Bitcoin received at these exchanges can be traced back to mining operations or exchanges not based in Iran, while substantial amounts of the outgoing Bitcoin can be ***traced to various exchanges located around the world.*** (Emphasis added.)

242. In February 2022, likewise, Chainalysis issued a public warning that “[s]ome in the Iranian government have called for the country to use cryptocurrency to circumvent [U.S.] sanctions,” “Iranian Bitcoin mining is well underway at a surprisingly large scale,” and “Iranian state actors are well aware of the opportunity.” Accordingly, this growth in the Iranian state’s focus on cryptocurrency has “opened up a new avenue of risk for cryptocurrency businesses” that may “face penalties or even criminal prosecution if found in violation of OFAC sanctions.” Cryptocurrency exchanges, such as Binance, should therefore “monitor for exposure to Iranian miners to reduce this risk considerably.”

243. In November 2022, moreover, Jonathan Levin, Chief Strategy Officer at Chainalysis, submitted formal comments to Treasury where he explained that “Iran stands out for its embrace of cryptocurrency. . . . Several generals in the Islamic Revolutionary Guard Corps (IRGC) — which plays an outsize role in Iran’s politics and economy and is designated as a

Foreign Terrorist Organization — have publicly endorsed the use of cryptocurrency, including the launch of a central bank digital currency, to circumvent sanctions.”

244. Defendants were generally aware of these warnings from blockchain analysis firms, each of which independently conveyed to Defendants that actors in the Government of Iran and the IRGC may seek to transact using cryptocurrency on its exchange and that they used cryptocurrency to fund their operations and commit terrorist attacks. Despite this general awareness, Defendants willfully disregarded AML/CFT requirements and enabled the IRGC and its affiliates to transact on the Binance.com exchange.

245. On information and belief, Defendants also received similar—but more detailed—nonpublic warnings from blockchain analysis firms with whom Binance had retained.

### **3. Warnings from Terrorism Scholars and NGOs**

246. Terrorism scholars and NGOs, similarly, warned that the IRGC sought to embrace cryptocurrency as a strategy for evading sanctions and funding terrorism. In January 2020, for example, Yaya Fanusie, an adjunct senior fellow at the Center for a New American Security, published an article in *Forbes* where he explained that “[t]he Iranian regime has stepped up its support for blockchain technology research, particularly after the U.S. reimposed sanctions on many Iranian banks . . . in 2018.”

247. In June 2021, likewise, Eric Lorber, of the Foundation for Defense of Democracies, testified before Congress that, “Iran has turned to bitcoin mining as one way to mitigate the impact of the restrictions on its oil sector” and “provide[] a way for Iranians to earn revenue” for which “it is estimated that the amount of bitcoin mined in Iran could equal approximately \$1 billion annually.” Accordingly, Lorber warned, “Iranian think tanks have recognized the potential for sanctions evasion, noting that bitcoin may not be traceable and can be used on international exchanges.”

248. In November 2022, similarly, following reports from *Reuters* that “Binance had processed \$7.8 billion worth of Iranian crypto transactions since 2018 despite extensive US financial sanctions against Tehran,” *Arab News* reported that “almost all the funds passed between Binance and Iran’s largest crypto exchange, Nobitex, which offers guidance on its website on how to skirt sanctions.” Interviewing several scholars, *Arab News* reported:

“Iran has increasingly utilized cryptocurrencies, and crypto mining, in recent years to evade US-imposed sanctions on its economy and to bolster domestic revenue with some success,” [Ali Plucinski, a cybersecurity analyst for the risk intelligence company RANE] told *Arab News*. . . . “After four decades of assorted sanctions, the Iranian government has perfected a variety of techniques for evading sanctions, and crypto is certainly one of its tools,” Barbara Slavin, the director of the Future of Iran Initiative and a non-resident senior fellow at the Atlantic Council, told *Arab News*. **“I would bet that the Islamic Revolutionary Guard Corps is behind these ‘illegal’ mining efforts,”** she said. **“I think *this is more a regime phenomenon* than something used by ordinary people who tend to stockpile dollars or consumer goods as a hedge against inflation.”** Plucinski pointed out that it is illegal “to buy, sell or invest in cryptocurrency in Iran, and crypto payments within the country are similarly illegal.” “Citizens can engage in crypto-mining practices that the Iranian government permits,” she said. “Crypto-mining for personal gain is prohibited and Iranian police have regularly engaged in crackdowns on illicit mining operations throughout the country.” The Iranian regime officially recognized crypto-mining in 2019. Miners were required to identify and register themselves, pay an electricity tariff, and sell their mined bitcoin to Iran’s central bank. “Iran’s shift to cryptocurrencies has ***proven to be quite effective for the regime in evading US sanctions***, evidenced by the recent article of Reuters,” Plucinski said. (Emphasis added.)

Moreover, quoting Ali Plucinski, *Arab News* explained that ““Iran has had significant success in finding alternate ways to bolster its economy through cryptocurrency production in spite of strong international sanctions,”” and the regime’s approval of the ““use of crypto funds to pay for imports in August 2022, thereby enabl[ed] the regime to circumvent extensive US sanctions imposed on Iran’s finance and banking sector.”” Indeed, the ““Iranian government has announced its intention to bolster foreign trade with specific countries through the use of cryptocurrencies and smart contracts.””

249. In February 2023, the Foundation for Defense of Democracies, a non-partisan NGO, warned that “[i]n January 2022, Iran directed its sanctioned central bank to expand its use of cryptocurrency. Then, in August, Tehran announced it approved cryptocurrency regulations, a sign that digital assets would pay for otherwise sanctionable imports. In fact, the regime pledged to use cryptocurrency as a medium for foreign trade to evade U.S. sanctions.”

250. Defendants were generally aware of these, and similar, warnings from scholars and NGOs, each of which independently conveyed to Defendants that actors in the Government of Iran and the IRGC may seek to transact using cryptocurrency on the Binance exchange and that they used cryptocurrency to fund their operations and commit terrorist attacks. Despite this general awareness, Defendants willfully disregarded AML/CFT requirements and enabled the IRGC and its affiliates to transact on the Binance.com exchange.

**C. Defendants Were Generally Aware That Hamas and PIJ Embraced Cryptocurrency to Fund Terrorist Attacks**

251. Both prior to Binance’s founding and throughout the events described in this Complaint, Defendants were generally aware that Hamas and PIJ sought to exploit cryptocurrency and cryptocurrency exchanges, like Binance, to sustain their campaign of terrorist attacks, including by supporting Hamas’s and PIJ’s terrorist attacks.

252. Before and throughout the Relevant Period, warnings of Hamas’s and PIJ’s embrace of cryptocurrency were legion and came from all sorts of bodies—including the U.S. government, blockchain analysis firms, terrorism scholars, and NGOs.

**1. Warnings from the U.S. Government**

253. The U.S. government issued warnings—including directly to cryptocurrency exchanges, like Binance—that alerted Defendants that Hamas and PIJ embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

254. In 2019, on the anniversary of 9/11, Under Secretary Mandelker gave a speech highlighting the growing risk of terrorist exploitation of cryptocurrencies—and the necessity of actors like Defendants implementing robust AML/CFT policies. As she explained, “without the appropriate strong safeguards cryptocurrencies could become the next frontier” for terrorists to use to transfer funds. And she highlighted a recent campaign by Hamas to “solicit bitcoin donations via social media.” Under Secretary Mandelker emphasized that even limited transfers of cryptocurrency to terrorists was extremely dangerous because “the cost of carrying out a terrorist attack can be very low”—indeed, a “FinCEN analysis found remittances linked to terrorism averaged less than \$600 per transaction.” She thus issued a call-to-action for the cryptocurrency industry: The “digital asset industry” “needs to harness [its] technological expertise and apply it to the tough problems we need to solve in illicit finance – both because not doing so *threatens national security*, and because it is the only way for them to pass regulatory muster.” (Emphasis added.)

255. Moreover, in summer 2020, DOJ announced the dismantling of a terrorist financing cyber-enabled campaign, involving the al-Qassam Brigades, Hamas’s operations arm. The Hamas campaign “relied on sophisticated cyber-tools, including the solicitation of cryptocurrency donations from around the world.” As DOJ explained, “[i]n the beginning of 2019, the al-Qassam Brigades posted a call on its social media page for bitcoin donations to fund its campaign of terror. The al-Qassam Brigades then moved this request to its official websites, alqassam.net, alqassam.ps, and qassam.ps.” Those “websites offered video instruction on how to anonymously make donations, in part by using unique bitcoin addresses generated for each individual donor.” The U.S. government ultimately “tracked and seized all 150 cryptocurrency accounts that laundered funds to and from the al-Qassam Brigades’ accounts.”

## 2. Warnings from Blockchain Analysis Firms

256. Analyses published by blockchain analysis firms, terrorism scholars, and NGOs alerted Defendants that Hamas and PIJ embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

257. For example, in April 2019, Elliptic warned that “[t]errorist organizations are increasingly experimenting with raising funds in cryptocurrencies. Their global reach and perceived anonymity make them an attractive mechanism for receiving donations to their cause. . . . In January of this year, the Al-Qassam Brigades, the military wing of Hamas, began such a fundraising campaign.”

258. Moreover, TRM Labs reported in July 2021 that “On July 1, 2021, the Israeli National Bureau of Counterterrorism Finance (NBCF), released a copy of an administrative seizure for Bitcoin, Doge, Tron, and other cryptocurrency addresses controlled by agents of Hamas.” TRM warned that “Since at least early 2019, the Izz-Al Din-Al Qassam Brigades, Hamas’ military arm, has attempted to use cryptocurrencies as an alternative fundraising method to support its military operations.”

259. Likewise, Chainalysis’s Global Head of Policy and Regulatory Affairs explained before Congress in 2021 that, “[r]ecently, a representative from Palestinian militant group Hamas confirmed that they have seen an increase in cryptocurrency donations. The group is able to use cryptocurrency to circumvent international sanctions to fund its military operations. This is not a new trend for the group, which has exploited cryptocurrency in the past to raise money.”

260. In July 2023, reporting on Israel’s seizure of dozens of cryptocurrency wallets associated with PIJ, Elliptic warned of PIJ’s embrace of cryptocurrency, explaining that “[w]ith this seizure order, the PIJ becomes the eighth known proscribed terrorist organization that has

engaged with cryptoassets, alongside other major groups such as ISIS, al-Qaeda, Hay'at Tahrir al-Sham (HTS), Hezbollah, Iran's Islamic Revolutionary Guard Corps (IRGC) and Hamas."

**D. Defendants Were Generally Aware That Al-Qaeda and ISIS Embraced Cryptocurrency to Fund Terrorist Attacks**

261. Both prior to Binance's founding and throughout the events described in this Complaint, Defendants were generally aware that al-Qaeda and ISIS sought to exploit cryptocurrency and cryptocurrency exchanges, like Binance, to sustain their campaign of terrorist attacks, including by supporting al-Qaeda's and ISIS's terrorist attacks.

262. Before and throughout the Relevant Period, warnings of al-Qaeda's and ISIS's embrace of cryptocurrency were legion and came from all sorts of bodies—including the U.S. government, blockchain analysis firms, terrorism scholars, and NGOs.

**1. Warnings from the U.S. Government**

263. The U.S. government issued warnings—including directly to cryptocurrency exchanges, like Binance—that alerted Defendants that al-Qaeda and ISIS embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

264. In 2015, Treasury warned in its *National Terrorism Financing Risk Assessment* that "virtual currencies such as Bitcoin and other emerging payments technologies . . . have attracted the attention of various criminal groups, and may be ***vulnerable to abuse by terrorist financiers***." (Emphasis added.) After discovering that "a blog linked to ISIL has proposed using Bitcoin to fund global jihadist efforts," Treasury warned that "[g]iven the attractiveness of virtual currency to conduct illicit financial transactions," "terrorist groups may use these new payment systems to transfer funds collected in the United States to terrorist groups and their supporters located outside of the United States." More broadly, according to Treasury, bad actors were attracted to cryptocurrencies because they offered "anonymity for both users and transactions;

the ability to move illicit proceeds from one country to another quickly; low volatility, which results in lower exchange risk; widespread adoption in the criminal underground; and trustworthiness.”

265. One such warning came from DOJ in October 2020: it had recently seized “hundreds of thousands of dollars’ worth of bitcoin” by “dismantling . . . terrorist financing campaigns . . . involving . . . al-Qaeda[] and ISIS.”

266. Another warning came from a 2020 report of the Lead Inspector General for Overseas Contingency Operations: “Treasury reported that ISIS continues to raise funds through extortion and oil smuggling networks in eastern Syria, ransoms from kidnappings, and the operation of front companies. . . . Treasury reported that ISIS increasingly relied on cryptocurrencies, with members transferring funds from Iraq to members in northeastern Syria, including in the al-Hol displacement camp.”

267. The Lead Inspector General for Overseas Contingency Operations similarly reported in 2021 that, according to Treasury, “ISIS supporters use cryptocurrencies and online fundraising platforms.”

268. In July 2021, likewise, John Eisert, Assistant Director for Investigative Programs, Homeland Security Investigations, at the Department of Homeland Security, testified before Congress: “[I]n 2020, [U.S. government agencies] initiated an investigation related to 24 cryptocurrency accounts, all of which were identified as foreign assets or sources of influence for al-Qaeda. This investigation was initiated to investigate the unlawful use of cryptocurrency to support and finance terrorism. As a result of this investigation, [the U.S. government] subsequently seized 60 virtual currency wallets used in this terrorism financing scheme.”

## 2. Warnings from the United Nations

269. The U.N. issued warnings that alerted Defendants that al-Qaeda and ISIS embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

270. For example, a 2016 U.N. Security Council report warned that “[a]s ISIL comes under continued pressure . . . it is likely that it will attempt to move funds internationally and to convert local currency into currency . . . which can be more easily transferred and used internationally. Money-service businesses, hawala exchange houses and other informal transfer systems remain vulnerable to abuse, but further attention should also be given to new payment methods, such as prepaid cards and virtual currencies. . . . Vigilance is essential not only to prevent ISIL from being able to maintain funds abroad but also to prevent it from distributing funds to its affiliates and facilitating attacks around the world.”

271. In 2021, moreover, the U.N. Security Council publicly warned that “Member State reporting on the use of cryptocurrencies in the financing of . . . Al-Qaida continues to grow. . . . Al-Qaida affiliates in the Syrian Arab Republic operated a bitcoin network using Telegram channels and other social media platforms to solicit cryptocurrency donations.”

272. In 2021, likewise, the U.N. Security Council published reports monitoring terrorist organizations that also “highlighted concerns about the growth in the use of cryptocurrencies by terrorists,” citing as examples the “successful prosecution[]” in France “of a terrorism finance case involving the use of cryptocurrencies” and a “recent case of an Al-Qaida bounty offered for the killing of police officers with the reward to be paid in bitcoin.” In addition, the U.N. warned that “virtual assets were used to evade sanctions and raise funds to support terrorism” in at least “100 case studies for the period 2017-2020,” and there were “ongoing reports of increased use of cryptocurrency by ISIL and Al-Qaida and terrorist fighters or their family members seeking to raise funds via cryptocurrency.”

273. A 2022 U.N. Security Council report likewise warned that ISIS “increasingly used virtual currencies, especially so-called stable coins, and continued to fundraise on social media platforms.”

274. Another 2022 U.N. report explained that “United Nations entities continued to support efforts to mitigate [ISIS]’s ability to generate resources for terrorism purposes,” including through “efforts to counter the use of virtual assets for terrorist financing purposes.” Per the U.N., ISIS “increasingly used new technologies, including . . . cryptocurrencies, as well as ICTs, including the Internet and social media platforms.”

### **3. Warnings From Blockchain Analysis Firms, Terrorism Scholars, and NGOs**

275. Analyses published by blockchain analysis firms, terrorism scholars, and NGOs alerted Defendants that al-Qaeda and ISIS embraced cryptocurrency to evade U.S. counterterrorism sanctions and fund attacks.

276. In 2017, Seamus Hughes, Deputy Director of the Program on Extremism at George Washington University, testified before Congress and explained that ISIS supporters have publicly “discussed the use of Bitcoin, a cryptocurrency, to fund IS[IS]” and shared “how-to” guides “of best practices for digital currency to use to support IS[IS].”

277. In 2018, for example, Ahmad Helmi Hasbi and Remy Mahzam, of the International Centre for Political Violence & Terrorism Research from the S. Rajaratnam School of International Studies, warned in an article: “The growing interest in cryptocurrencies in extremist networks is evidenced by the inclusion of a Tech Talk section in a recent issue of ‘Al-Haqiqa’, a pro-Al-Qaeda English-language magazine released in February 2018 which examines the *Shari’ah* or Islamic law permissibility of using Bitcoins and other cryptocurrencies to fund their jihadist pursuits. . . . Anti-terrorism hacktivist Ghost Security Group had previously

disclosed that the 2015 Charlie Hebdo attack in Paris was funded by Al Qaeda in the Arabian Peninsula (AQAP) through Bitcoin financing.”

278. In June 2021, similarly, Chainalysis’s Global Head of Policy and Regulatory Affairs testified before Congress that “Al-Qaeda . . . operated a cryptocurrency terror finance campaign, evading U.S. sanctions” that was “conducted using Telegram and other social media platforms to solicit donations to fund violent terrorist attacks and equip terrorists in Syria. U.S. law enforcement was able to identify 155 virtual currency addresses associated with the terrorist campaign.” Indeed, several “al-Qaeda-affiliated groups” solicited funds through cryptocurrency and then sent “the proceeds on to al-Qaeda’s BitcoinTransfer addresses.” According to a report from CipherTrace in 2021, al-Qaeda’s campaign raised hundreds of thousands of dollars for al-Qaeda and affiliated terrorist groups to commit terrorist attacks.

279. Similarly, Eric Lorber, of the Foundation for Defense of Democracies, testified before Congress in summer 2021 that “[o]ne area of concern in addition is the cryptocurrency space where we have seen rogues like . . . al-Qaida . . . increasingly utilize crypto assets to evade sanctions.”

280. As scholar William Vlcek wrote in 2022, “As IS lost territory, it appears that the leadership sought to secure the future of the organization and retain as much of their accumulated financial assets as possible. Interviews with some of the people connected to exchange houses located outside of IS territory highlighted what they saw as a concerted effort by the group to shift money out of the region, . . . consistent with what one author has identified as a ‘boom-bust’ cycle of organizational existence among insurgent groups (Ahmad 2021). The logic derived from this study of jihadist groups is, in some ways, like the business cycle for an economic sector. When times are good the organization builds up its economic reserves, and

these reserves in turn help the organization to survive the lean times of the ‘bust’ phase of the cycle. . . . [t]he US Department of Justice seized cryptocurrency wallets connected with terrorist financing for IS . . . [while] IS [was] operating as an insurgent group seeking to . . . undertake further terrorist attacks outside of the Middle East.”

**E. Defendants Disregarded Voluminous Warnings That Operating an Illegal Money Transmittal Business and Defying U.S. AML/CFT and KYC Rules Foreseeably Aided Attacks by the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, and ISIS**

281. Through a litany of warnings—namely from the U.S. government—Defendants knew of the importance of cryptocurrency exchanges, such as Binance, establishing and enforcing robust AML/CFT and KYC policies and procedures to counter the financing of terrorism. In 2013, for example, the Acting Assistant Attorney General for the Criminal Division testified to Congress that DOJ “anticipates that virtual currency will continue to evolve and grow in popularity. . . . As members of the U.S. financial community, virtual currency services can and must safeguard themselves from exploitation by criminals and terrorists by implementing legally required anti-money laundering and know-your-customer controls.”

282. In 2015, likewise, Treasury observed that, by reporting suspicious activity, financial institutions helped “reduced the funding available for terrorist operations and have made the concealment and transfer of terrorism related funds more difficult. . . . The reporting unmask[s] the relationships between possible terrorist groups and their financing networks, enabling law enforcement to target the underlying conduct of concern, and to use forfeiture and sanctions to disrupt their ability to operate and finance their activities.”

283. In February 2018, Treasury Under Secretary Mandelker warned that “compliance work conducted by the private sector . . . are critically important to stopping the flow of funds to weapons proliferators like . . . Iran, [and] terrorist[] organizations like ISIS and Hizballah”

because “[i]llicit actors continuously seek out the weakest links in the chain” and therefore “[b]usinesses that let their guard down make it easier for criminals to access and abuse our markets to further their illicit aims.” Under Secretary Mandelker also warned how “[c]ritical . . . the regulatory framework and enforcement authorities we have in place that govern the use of virtual currency” was to prevent “illicit financing risks.” Thus, “[t]hrough FinCEN, Treasury regulates virtual currency exchangers as money transmitters and requires them to abide by Bank Secrecy Act obligations” and uses “strong enforcement powers to target those who fail to live up to their responsibilities.” Treasury remained committed, she explained, to ensuring that firms “dealing in virtual currency appropriately address their AML/CFT BSA responsibilities.”

284. In May 2019, FinCEN issued a detailed *Advisory on Illicit Activity Involving Convertible Virtual Currency*, for cryptocurrency exchanges, like Binance, and other financial institutions; the advisory directly addressed the prominent typologies and red flags associated with how bad actors use cryptocurrency. As FinCEN explained, cryptocurrencies create “terrorist financing” and other “illicit finance vulnerabilities due to the global nature, distributed structure, limited transparency, and speed of the most widely utilized virtual currency systems.” Thus, when a financial institution or cryptocurrency exchange “fails to comply with its AML/CFT program, recordkeeping and reporting obligations, as well as other regulatory obligations, such as those administered by” OFAC, that “risks exposing the financial system to greater illicit finance risks,” and risks exposing their services to “being leveraged in money laundering, terrorist financing, and other related illicit activities.” Indeed, without “sufficient AML/CFT controls,” exchanges and cryptocurrencies become “an attractive method of money transmission by those engaged in illicit conduct and other criminal acts that threaten U.S. national security,” including “terrorist financing,” and “sanctions evasion.” FinCEN even gave concrete directives

to cryptocurrency exchanges, like Binance: “Businesses and entities dealing in digital currency should implement policies and procedures that allow them to: block IP addresses associated with a sanctioned country or region; disable the accounts of all holders identified from a sanctioned country or region; install a dedicated Compliance Officer with authority to ensure compliance with all OFAC-administered sanctions programs; screen all prospective users to ensure they are not from geographic regions subject to U.S. sanctions; and ensure OFAC compliance training for all relevant personnel.”

285. In May 2019, Treasury Under Secretary Mandelker similarly warned cryptocurrency exchanges during a widely publicized industry event that “AML/CFT and sanctions expectations for the digital currency industry. . . . [s]hould be viewed as a duty serving our national security” and businesses need to be “built on a strong foundation of anti-money laundering and sanctions compliance from the very beginning.” Indeed, according to the Under Secretary, the “features of emerging technologies that appeal most to users and businesses – like speed of transfers, rapid settlement, global reach, and increased anonymity – can also create opportunities for rogue regimes and terrorists. It is for this reason that industry compliance with our regulations is so critical.” Bottom line: “Nobody here wants to see innovative products and services misused to support terrorism and weapons proliferation.”

286. During that same speech to industry participants, Under Secretary Mandelker emphasized the importance of reporting suspicious activity to Treasury—and she even lauded the cryptocurrency industry for its performance in reporting such suspicious activity. As the Under Secretary explained:

[Businesses] are not only doing this to comply with our regulatory expectations, but also to make sure you are not the next business that North Korea or Hamas or narcotraffickers exploit. We have found great partners in your industry committed to this objective. Since 2013, FinCEN has received over 47,000 suspicious activity reports (SARs) mentioning

bitcoin or virtual currency more broadly. Half of these SARs were *filed by virtual currency exchangers or administrators themselves*. These filings have been critical to law enforcement efforts.

287. Identifying suspicious activity was ***not***, the Under Secretary clarified, limited to “run[ning] a check of names against OFAC’s [sanctions] lists,” as that could “miss other prohibited activity.” Instead, compliance programs should “be dynamic.” Indeed, “the best compliance programs are those that incorporate red flags and typologies into their programs to protect their businesses, and then use this information to provide reporting back to [Treasury], as appropriate, including through suspicious activity reports. In addition, OFAC’s sanctions programs target not just specific individuals and entities, but ***also whole jurisdictions***, such as Cuba, ***Iran***, North Korea, and Syria.” (Emphasis added.)

288. In July 2019, Treasury Secretary Mnuchin warned that “Treasury has been very clear to . . . providers of digital financial services that they must implement the same anti-money laundering and countering financing of terrorism -- known as AML/CFT -- safeguards as traditional financial institutions.”

289. In November 2019, during the Chainalysis blockchain symposium, FinCEN Director Kenneth Blanco explained the importance of regulatory compliance and suspicious activity reporting to preventing terrorism:

We use the information you provide to save lives and protect people and our national security. These are not just rules that we are requiring you to comply with — there is a good reason for them, and they have an important purpose. They protect people and save lives; this is a national security issue. . . . ***It is important to the person who lost a loved one to an act of terror***, . . . [c]ompliance—by financial institutions in particular—plays a critical role in preventing these tragedies from occurring. In many instances, ***they are the first line of defense***. (Emphasis added.)

290. In that same November 2019 speech, Director Blanco explained that FinCEN uses SARs “provided by financial institutions to identify illicit finance trends, methodologies, and

typologies to inform law enforcement agents, prosecutors, regulators, and others about how convertible virtual currency is used by criminals including terrorists, rogue states, and other bad actors. This allows them to think about how to fill the gaps and vulnerabilities that put our nation and its people at risk, while also preventing crime before it happens or preventing it from spreading once it has occurred.”

291. In 2020, DOJ warned that “the explosion of . . . exchanges that use cryptocurrency may provide . . . terrorists with new opportunities to transfer illicitly obtained money” and that bad actors may “attempt to hide financial activity by using cryptocurrency exchanges that do not comply with internationally recognized [AML] and combating the financing of terrorism [CFT] standards.” DOJ was emphasized that “exchanges can serve as a *haven for criminal activity by operating under lax rules or by flouting AML protocols*. In the normal course, registered exchanges that comply with AML standards and [KYC] requirements are likely to possess relevant transactional information. However, exchanges that avoid compliance with such requirements provide criminals and *terrorists* with opportunities to hide their illicit financial activity from regulators and investigators.” (Emphasis added.)

292. On information and belief, U.S. government agencies and high-ranking officials also directly warned Defendants about establishing and enforcing robust AML/CFT and KYC policies and procedures to counter the financing of terrorism.

**F. Defendants Disregarded Voluminous Warnings That Processing Transactions for Customers in Violation of U.S. Counterterrorism Sanctions, Including U.S. Countrywide Sanctions, Targeting Iran, Syria, the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, or ISIS Foreseeably Aided Terrorist Attacks**

293. Through a litany of warnings—namely from the U.S. government—Defendants knew that processing transactions for customers in violation of U.S. sanctions, including U.S.

countrywide sanctions, targeting Iran, Syria, the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, or ISIS foreseeably aided terrorist attacks.

294. As the White House made crystal clear in January 2018: “The Iranian regime is the world’s leading state sponsor of terror. It enables Hezbollah, Hamas, and many other terrorists to ... kill innocent people. It has funded, armed, and trained more than 100,000 militants to spread destruction across the Middle East. ... We are cutting off the regime’s money flows to terrorists. We have sanctioned nearly 100 individuals and entities involved with the Iranian regime’s ballistic missile program and its other illicit activities. ... We are also supporting [] brave Iranian[s] ... who are demanding change from a corrupt regime that wastes the Iranian people’s money on ... terrorism abroad. ... [O]ur allies should cut off funding to the Islamic Revolutionary Guard Corps, its militant proxies, and anyone else who contributes to Iran’s support for terrorism. ... And they should not do business with groups that ... fund the Revolutionary Guard and its terrorist proxies.”

295. In 2020, the State Department explained how sanctions on Iran and the IRGC constrain their ability to commit and sponsor terrorist attacks, including by proxies:

The Iranian regime and its proxies continued to plot and commit terrorist attacks on a global scale. In the past, Tehran has spent as much as \$700 million per year to support terrorist groups, including Hizballah and Hamas, though its ability to provide financial support in 2019 was ***constrained by crippling U.S. sanctions***. ... Tehran also continued to permit an al-Qa’ida (AQ) facilitation network to operate in Iran, sending money and fighters to conflict zones in Afghanistan and Syria, and it still allowed AQ members to reside in the country. Finally, the Iranian regime continued to foment violence, both directly and through proxies, in Bahrain, Iraq, Lebanon, Syria, and Yemen. .... Through the IRGC-QF, Iran continued its support to several U.S.-designated terrorist groups, providing funding, training, weapons, and equipment. Among the groups receiving support from Iran are Hizballah, Hamas, Palestine Islamic Jihad, Kata’ib Hizballah (KH) in Iraq, ... the Houthis in Yemen, and [] the Taliban in Afghanistan. (Emphasis added.)

296. As Treasury’s Deputy Assistant Secretary for Terrorist Financing and Financial Crimes Daniel Glaser explained in 2016, “[t]argeted financial sanctions not only deprive terrorist organizations of funds that are necessary to carry out their harmful activities, but force these groups to devote additional time and resources to seek out new sources of funding and channels to move funds.”

297. Indeed, in 2021, Treasury explained that its sanctions efforts “have *disrupted the Iranian regime’s ability to fund* its broad range of malign activities, including supporting its proxies Hizballah and Hamas,” including “by sanctioning over 700 individuals, entities, aircraft, and vessels” and imposing “a variety of targeted financial measures that disrupt funding sources such as oil, its primary source of funds, as well as other areas such as banking, petrochemicals, shipping, and metals.” Treasury’s “sanctions on the Iranian regime . . . reduce Iran’s capacity to continue its support for terrorism, human rights abuses, ballistic missile proliferation, destabilizing activities, and support of militant groups.” (Emphasis added.)

298. Treasury in 2018 explained that its imposition of “sanctions on the Iranian regime . . . . [a]re designed to greatly reduce Iran’s capacity to continue its support for terrorism, human rights abuses, ballistic missile proliferation, destabilizing activities, and support of militant groups.” Treasury is using those “financial tools” to disrupt the funding and support for groups such as “the Islamic State of Iraq and Syria (ISIS), al-Qaida, Hizballah, Hamas, the Taliban and others.”

299. Former State Department employee Gabriel Noronha explained in 2023 that U.S. sanctions on Iran directly reduce the regime’s ability to fund terrorist attacks by its proxies, including Hamas: “In 2018, the State Department disclosed that Iran was providing Palestinian terror groups, including Hamas, with \$100 million per year,” but “[i]n 2019, after the United

States reimposed sanctions on Iran, the regime's available funds for terrorism declined and Hamas was forced to institute an 'austerity plan.'"

300. Defendants, however, disregarded these warnings when they processed voluminous transactions for FTOs, including the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, and ISIS, on the Binance exchange.

301. On information and belief, U.S. government agencies and high-ranking officials also directly warned Defendants that processing transactions for customers in violation of U.S. sanctions, including U.S. countrywide sanctions, targeting Iran, Syria, the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, Al-Qaeda, or ISIS foreseeably aided terrorist attacks.

**V. Defendants Knowingly Enabled Foreign Terrorist Organizations And Their Affiliates To Transact On The Binance Exchange**

302. Defendants acted with a highly culpable state of mind. In many cases, Defendants had actual knowledge that their conduct was enabling terrorist violence, and that they were violating laws designed to prevent terrorist attacks against Americans. Indeed, in many cases, Defendants had specific information about the users and transactions it was enabling revealing their prohibited nature—but they willfully enabled those users and transactions anyway.

303. The inference of a culpable state of mind is especially strong in this case because none of Defendants' culpable conduct constituted routine business activity. Instead, Defendants knowingly and intentionally deviated from all norms of routine business behavior when they facilitated transactions and withdrawals for FTOs, their supporters, and their agents. That is why Defendants were found criminally liable, and forced to execute settlements with multiple government agencies responsible for regulating the financial sector.

**A. Defendants' Admissions**

304. In their settlement agreements and guilty pleas, Defendants admitted that they knew that designated terrorists and state sponsors of terrorism, including the Iranian regime, transacted on the Binance.com platform. Indeed, Defendants' admitted culpability is historic: as Treasury reported to Congress in the *2024 National Terrorist Financing Risk Assessment*, when "Binance settled with FinCEN and OFAC for violations of AML and sanctions laws, each assess[ed] the largest civil monetary penalty in their history":

Binance did business as a money transmitter in substantial part within the United States, including by cultivating and serving over 1 million U.S. customers through its main platform, but at no time did Binance register with FinCEN. Additionally, Binance failed to file SARs with FinCEN on significant sums being transmitted to and from entities officially designated as terrorist organizations by the United States and United Nations, as well as high-risk exchanges associated with terrorist financing activity. Binance user addresses were found to interact with bitcoin wallets associated with ISIS, Hamas' Al-Qassam Brigades, Al Qaeda, and the Palestinian Islamic Jihad (PIJ).

305. Binance knew that its policies enabled crime and terrorist finance. In a September 2018 chat conversation, a senior Binance employee learned that Binance had "[n]othing . . . in place" to review high-volume accounts for suspicious activity. In the same chat, he listed types of transactions that, "in [the] aml world," would be flagged for money laundering risks. Binance, however, did not have protocols to flag or report such transactions. The senior employee further noted: "its [sic] challenging to use the aml standards to impose on [Binance].com especially when Cz [Zhao] doesn't see a need to."

306. In February 2019, after receiving information "regarding HAMAS transactions," on Binance, the Chief Compliance Officer explained to a colleague that "terrorists usually send

‘small sums’ as ‘large sums constitute money laundering.’” The colleague wryly replied: “can barely buy an AK47 with 600 bucks.”

307. In a chat conversation around the same time, one compliance employee wrote that Binance needed “a banner” that stated, “is washing drug money too hard these days - come to Binance we got cake for you.” And in another chat a year later, the Chief Compliance Officer commented of various Binance users: “Like come on. They are here for crime.” Binance’s Money Laundering Reporting Officer agreed, saying, “we see the bad, but we close 2 eyes.”

308. Indeed, Defendants took steps to *retain* known illicit actors on the Binance platform, particularly if they were VIP users. For example, in July 2020, Binance’s then-CFO and others discussed a VIP user who was offboarded after being publicly identified as among the “top contributors to illicit activity.” The CFO wrote that, as a general matter, Binance’s compliance and investigation teams should check a user’s VIP level before offboarding them, and then Binance could “give them a new account (if they are important/VIP)” with the instructions “not to go through XXX channel again.”

309. Similarly, when a third-party provider alerted Binance in April 2019 of Hamas-associated transactions on Binance.com, Binance did not take actions against the transactors; instead, it attempted to influence the third-party service provider that reported on Binance’s conduct, attempting to conceal the wrongdoing.

310. In other cases, Binance took action to help terrorist financiers escape scrutiny or keep their funds. Thus, in July 2020, when a third-party service provider flagged accounts associated with the terrorist groups ISIS and Hamas, Binance’s former Chief Compliance Officer instructed personnel to “[c]heck if he is a VIP account, if yes, to . . . [o]ffboard the user but let him take his funds and leave. Tell him that third party compliance tools flagged him.” The

individual was allowed to keep an account for several years in withdrawal-only status after the designation and withdraw the balance.

311. That interaction was part of a pattern. Indeed, Binance had a policy stating that for VIP customers, if law enforcement requested the freezing of an account, then as soon as the account was unfrozen, the VIP team was to contact the user “through all available means (text, phone) to inform him/her that his account has been frozen or unfrozen. Do not directly tell the user to run, just tell them their account has been unfrozen and it was investigated by XXX. If the user is a big trader, or a smart one, he/she will get the hint.”

312. Even though Defendants knew for years that prohibited users were using Binance.com, Binance refused to take even minimally effective steps to prevent that use. This is because Zhao personally believed that implementing robust KYC requirements would deter users from joining Binance’s platform, thus decreasing Binance’s transaction volume and therefore its revenues. Defendants thus maintained a deliberately ineffective KYC and blocking policy precisely so that Binance could court prohibited customers who otherwise would avoid the platform. That deliberate policy choice directly enabled Hamas, Hezbollah, PIJ, and the IRGC to use the Binance platform to fund and commit terrorist attacks on Americans, including Plaintiffs.

#### **B. Defendants’ Consciousness of Guilt**

313. U.S. regulatory agencies determined, and Defendants’ conduct confirms, that Binance and Zhao were at all times conscious of the illegality and wrongfulness of their conduct. For example, U.S. regulators determined that:

- a. “Binance knew that its conduct constituted, or likely constituted, a violation of U.S. law when it intentionally retained both sanctioned jurisdiction users and U.S. users on its platform while understanding the applicability of U.S. sanctions to trades in which Binance matched U.S. and sanctioned jurisdiction users as counterparties. Binance’s knowledge that matching and executing trades between such users could cause the violation of sanctions is reflected in the statements of senior executives at the highest levels of the company, including the CEO and the

then CCO. The company's steps to encourage the circumvention of its controls further reflect the company's knowledge of the applicability of U.S. sanctions to its conduct."

- b. "Based on the large number of U.S. users on Binance.com and the liquidity they provided for its global trading activity, Binance knew, or had reason to know, its matching engines were routinely matching U.S. users with users from sanctioned jurisdictions over many years and at significant volumes. Such matches were inevitable in light of the trading volumes at issue, and Binance personnel were aware of the presence of each group and their trading activities on the exchange."
- c. "Despite awareness of Binance's failure to implement sufficient controls, Binance senior management mischaracterized its sanctions controls and its commitment to compliance to third parties in private communications, and to the public through actions such as issuing misleading Terms of Use and by removing references to sanctioned countries from its website when, in fact, it continued to serve them. It also encouraged the use of VPNs and surreptitiously allowed U.S. users and sanctioned jurisdiction users to trade even after ostensibly blocking them. For example, Binance continued to allow trades by users who were logged in from an IP address in a comprehensively sanctioned jurisdiction so long as that user had submitted KYC documents from a non-sanctioned jurisdiction."
- d. "Binance senior management not only allowed violations to persist for a prolonged period, but was also complicit in the misconduct. Binance's senior management was aware of its obligation to register as an MSB, but instead of complying with this obligation, directed Binance personnel to obscure the nature and extent of its ties to the United States. Similarly, Binance senior management was aware of the ineffective nature of its AML program and that illicit actors were exploiting Binance's AML weaknesses to effect suspicious transactions. Instead of addressing these AML deficiencies, senior management instructed Binance personnel to not file SARs and to obstruct law enforcement investigations. Binance was also not forthcoming about the ongoing nature of its registration-related violations that continued on the platform even well after FinCEN initiated its investigation."

314. Zhao, of course, was the most senior member of the "senior management" whose knowing misdeeds are described by the U.S. regulators above. As DOJ explained, "Zhao's willful violation of U.S. law was no accident or oversight. He made a business decision that violating U.S. law was the best way to attract users, build his company, and line his pockets. Despite knowing Binance was required to comply with U.S. law, Zhao chose not to register the company with U.S. regulators; he chose not to comply with fundamental U.S. anti-money-

laundering (AML) requirements; he chose not to implement and maintain an effective know-your-customer (KYC) system, which prevented effective transaction monitoring and allowed suspicious and criminal users to transact through Binance; and even when Binance employees detected suspicious transactions, Zhao's choices meant those transactions were not reported to U.S. authorities. And when it became clear that Binance had a critical mass of lucrative U.S. customers, Zhao directed Binance employees in a sophisticated scheme to disguise their customers' locations in an effort to deceive regulators about Binance's client base. ***Critically, Zhao knew that his decision not to implement an effective AML program would result in Binance facilitating transactions between U.S. users and users in Iran and other sanctioned countries and regions in violation of U.S. law.***" (Emphasis added.)

315. Senior Binance personnel repeatedly made statements and engaged in conduct that confirms their consciousness of guilt. As early as 2018, then-Chief Compliance Officer Samuel Lim said in an internal chat that "there is no fking way we are clean," admitted that Binance's customer service employees were "teaching ppl how to circumvent sanctions" and openly worried about "land[ing] in jail." In another, later chat, he acknowledged that Binance's users were "here for crime." Other Binance executives joked about the ease of using Binance.com to "wash[] drug money" and admitted that the company "see[s] the bad, but close[s] 2 eyes" and does nothing to prevent it.

316. Some of the "bad" that Binance and Zhao saw—but chose not to prevent—involved the use of the Binance.com exchange by Hamas, ISIS, and other terrorist groups.

317. Binance and Zhao destroyed documents related to illegal conduct, demonstrating their awareness that their conduct was wrongful and would subject them to legal liability.

318. The Defendants' consciousness of their guilt is relevant evidence of the consciousness and culpability of their misconduct, which foreseeably led to the terrorist attacks on Plaintiffs.

**C. Blockchain Analysis Software and Warnings from Third Parties**

319. Defendants learned in real-time, or close to it, from blockchain analysis software when terrorists, state sponsors of terrorism, and other bad actors were transacting on the Binance exchange. Despite that monitoring software, Defendants chose to *willfully ignore*, and to *continue processing*, transactions by terrorists and their supporters on the Binance exchange.

320. Defendants loudly touted Binance's compliance program and relationships with an army of third party blockchain analysis services as ways that gave Defendants robust insight into those who transacted on the Binance exchange. Indeed, Binance publicly represented that detailed, transaction- and customer-specific information from these analytic tools gave the insight necessary for complying with AML/CFT laws:

We invest heavily in KYC (Know Your Customer) and transaction monitoring technology with some of the strictest protocols in the industry. Unlike many other exchanges out there, we do not allow users to trade on our platform without passing KYC checks that include country of residence and personal ID information. One area in particular that we have ramped up is transaction monitoring. This is a dynamic process that utilizes the latest technology to *keep an eye on every transaction* to ensure that we can, *in real-time, discover and halt any illicit transactions and transfers*. To achieve this, we work with *partners* such as Chainalysis, TRM Labs, CipherTrace by Mastercard and Elliptic, as well as a *robust suite of internal tools*. (Emphasis added.)

321. Thus, Defendants had granular, real-time information on a transaction-by-transaction basis that terrorists and other bad actors were transacting on the Binance exchange.

322. Based on Defendants' own public statements, from the company's founding, Defendants used blockchain analysis tools, KYC, and AML/CFT tools, including proprietary tools, to monitor and identify those users who transacted on the Binance exchange. Through

those monitoring tools, Defendants knew the identities of users, including designated terrorists, who were operating on the Binance exchange.

323. In addition to Binance’s suite of internal tools, Binance partnered with several third-party analytics providers whose software and other monitoring tools informed Binance in real-time that terrorists were transacting on the Binance exchange. Each of these providers’ services informed Binance of terrorists operating on its exchange. Indeed, several providers—such as Chainalysis, CipherTrace, and Elliptic—regularly issued public reports that detailed terrorists’ use of cryptocurrency. Given Binance’s prior statements, such public blockchain analysis reports represent only a fraction of the *private* information that those providers shared with Binance. What follows is a non-exhaustive list of the third-party providers that Defendants engaged for AML/CFT purposes.

324. **Chainalysis**. No later than October 2018, Binance partnered with leading blockchain analysis and cryptocurrency compliance software provider Chainalysis. Through its partnership with Chainalysis, Binance developed and implemented purportedly “world-class AML compliance programs.” Chainalysis’s “compliance software, Chainalysis KYT (‘Know Your Transaction’)” offered a “real-time transaction monitoring solution for cryptocurrencies” by using “pattern recognition, proprietary algorithms and millions of open source references to identify and categorize thousands of cryptocurrency services to raise live alerts on transactions involved in suspicious activity.” Chainalysis’s “best-in-class” software enabled “cryptocurrency businesses,” like Binance, to “comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.” Chainalysis’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange. Chainalysis, for example, could “automatically

monitor for transactional exposure to Iranian entities with Chainalysis KYT”—a tool that helped cryptocurrency exchanges, like Binance, “avoid the risk of sanctions violations,” according to Chainalysis.

325. **Refinitiv**. No later than November 2018, Binance retained the financial software firm Refinitiv to implement an “automated Know Your Customer (KYC) application” that allowed “Binance to streamline the screening process for onboarding, KYC, and third-party risk due diligence.” That tool helped Binance ensure ““that anyone moving cryptocurrency into fiat currency is subject to the same KYC requirements as individuals dealing with a conventional bank.”” Refinitiv’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

326. **IdentityMind**. No later than March 2019, Binance “partnered with risk management and compliance firm IdentityMind,” to improve “compliance measures for Binance’s global operations by enabling IdentityMind’s tools for Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance.” IdentityMind’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

327. **CipherTrace**. No later than April 2019, Binance partnered with CipherTrace to “enhance the exchange’s robust anti-money laundering (AML) compliance program” and “raise Binance’s compliance standards,” per Binance. Binance’s former Chief Compliance Officer claimed the partnership would “bolster [Binance’s] existing world-class AML compliance program,” by using CipherTrace’s “cryptocurrency Anti-Money Laundering, cryptocurrency forensics, blockchain threat intelligence and regulatory monitoring solutions” to better allow

Binance to “assess and monitor threats.” CipherTrace’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

328. **Elliptic**. No later than May 2019, Binance “partnered with blockchain monitoring solutions provider Elliptic to boost its regulatory compliance”—specifically, its “Anti-Money Laundering” program. Elliptic’s tools enabled “blockchain-based transaction screening,” which allowed Defendants “to identify whether transactions are linked to illicit actors such as terrorist organizations.” As Elliptic claimed, “[b]y quickly identifying these addresses, [Elliptic’s tools would] ensure that [its] clients”—such as Binance—“are always aware of such links, and that we can meet their anti-money laundering and countering terrorist financing obligations.” Elliptic’s software, for example, enabled cryptocurrency exchanges—like Binance—to “proactively check future transactions for links to . . . terrorist fundraising wallets.” Elliptic’s tools necessarily alerted Defendants when IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

329. **Coinfirm**. No later than October 2019, Binance partnered with “international regulation technology company Coinfirm” to further “ensure it is compliant with the FATF regulations” about cryptocurrency AML/CFT rules. According to Binance’s Chief Compliance Officer, the partnership with Coinfirm ensured ““a comprehensive risk framework that balances user protection and user experience while complying with the FATF’s AML guidelines” thanks to Coinfirm’s “wide blockchain coverage and proprietary algorithms that cover more than 300 risk scenarios in real-time.” Coinfirm’s tools necessarily alerted Defendants when IRGC,

Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists were transacting on, or attempting to access, the Binance exchange.

330. On information and belief, Defendants used each of these blockchain-analysis tools independently—and certainly in the aggregate, especially when combined with Binance’s proprietary compliance software—to receive detailed real-time (or near-real-time) information about the identities, specific FTO affiliations, sanction status, geographies (*i.e.*, IP addresses), and counterparties involved in transactions on Binance exchange. Defendants, therefore, knew when terrorists accessed and transacted on the Binance exchange.

331. To be clear, despite the voluminous, highly detailed warnings that Defendants received about IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS terrorists, such FTOs’ supporters, or individuals from comprehensively sanctioned jurisdictions identified as a jurisdiction of primary money laundering concern, like Iran, transacting on the Binance exchange, Defendants took zero or minimal steps to halt those illicit transactions, effectively remove such FTOs or their supporters from the Binance exchange, or even report those illicit transactions to law enforcement or regulatory authorities. Instead, Defendants chose to knowingly process those illicit transactions.

**D. Alternatively, Defendants Willfully Blinded Themselves to the Enormous Volume of Transactions on the Binance Exchange That Enabled FTOs To Carry Out Terrorist Attacks**

332. To the extent Binance lacked information about a particular party or transaction, that lack of awareness can only be explained as willful blindness.

333. As the government’s findings show, Binance easily could have obtained the relevant information (as its third-party service providers, and even unrelated third parties often did). It could have implemented an effective KYC program. And it could have effectively screened transactions for sanctions compliance. Indeed, the law required Binance to take all of

these steps as a prerequisite to doing business with U.S. customers. Had Binance taken those basic steps to inform itself of the nature of its customers and their transactions, it would have quickly learned (to the extent it did not already know) that it was systematically enabling terrorist finance for designated FTOs and state sponsors of terrorism. Binance's refusal to inform itself constitutes willful blindness on par with actual knowledge.

334. The U.S. regularly publicly warned persons like Defendants in real-time that a willfully blind business model concerning Iran's countrywide sanctions and IRGC-facing sanctions *guaranteed* that such persons' Iran-related transactions foreseeably financed IRGC-sponsored attacks. In June 2010, for example, Treasury Under Secretary Levey testified before Congress as follows:

[W]e're working with countries to ensure that they take actions to fulfill for example the Financial Action Task Force's call for countermeasures against Iran. Iran remains the only country in the world subject to such a call for countermeasures.

But perhaps as important as all the governmental action is the second front of our strategy, the role of the private sector. As we have targeted Iran's illicit conduct, we have also taken public action and made an unprecedented effort to share the information that forms the basis of our actions with firms all over the world. We have made that evidence public to the extent possible.

That information demonstrates that Iran engages in illicit nuclear and ballistic missile transactions, supports terrorist groups and that, in order to conduct those activities, engages -- it engages in financial deception designed to evade the controls of responsible businesses that have no desire to participate in illicit activity. In response to this information and to protect their own reputations, virtually all major financial institutions have either completely cut off or dramatically reduced their ties with Iran. We are now starting to see other companies across a range of sectors, including insurance, consulting, energy and manufacturing, making similar decisions. ...

[O]f course, as this committee knows, there's ample information in the public domain to establish that Iran uses its banks and abuses the financial services of other banks for precisely those illicit purposes. We have also repeatedly revealed the mechanisms by which Iranian banks seek to mask their misconduct. This includes stripping their names from transactions, disguising the

ownership of assets on their books and using non-sanctioned banks to stand in the shoes of sanctioned ones.

***Given this record, it would be nearly impossible for financial institutions and governments to assure themselves that transactions with Iran are not being used to contribute to nuclear missile industries. ...***

We have now designated 26 IRGC-related entities, including the IRGC's Qods Force, for providing material support to the Taliban, Hezbollah, Hamas, the Palestinian Islamic Jihad and others. (Emphasis added.)

335. In September 2010, similarly, Under Secretary Levey publicly warned that given the unique nature of Iran's government, IRGC, and counterterrorism regime, a person did not need to know anything more than the fact that a financial transaction went to Iran to conclude that it more likely than not enabled IRGC violence:

***Today, Iran is effectively unable to access financial services from reputable banks*** and is increasingly unable to conduct major transactions in dollars or Euros. ... Iran is now struggling to mitigate the effects of sanctions. Iran's leaders are turning increasingly to the [ ] IRGC – Iran's military vanguard that has long been involved in Iran's terrorism and missile programs – to prop up the economy. This is likely to exacerbate Iran's isolation, as companies around the world have begun to shun all business with the IRGC. ... ***Because many in the private sector are simply unable to distinguish between Iran's legitimate and illicit transactions, they have opted to cut off Iran entirely. ...***

UNSCR [U.N. Security Council Resolution] 1929 contains a ... requirement to exercise vigilance when conducting business with any Iranian entity including the IRGC .... The Resolution's financial provisions call upon member states to prevent all financial services (including banking, insurance and reinsurance) if there are reasonable grounds to believe that such services could contribute to Iran's ... missile programs.

Significantly, the language of these provisions provides a legal basis for member states to take strong steps. ***And given the strong public record regarding Iran's illicit and deceptive activities, the operating presumption should be that virtually all transactions or financial services involving Iran could contribute to its ... missile programs.*** (Emphasis added.)

336. In January 2018, likewise, Treasury Under Secretary Mandelker publicly warned during testimony before Congress as follows:

Iran is [a] rogue regime that seeks to subvert the financial system. It is the leading state sponsor of terrorism and finances terrorist groups such as Hizballah and Hamas, and ... Shi'a militant groups in ... Iraq ....

Like North Korea, Iran uses deceptive financial practices to generate revenue. As just one example, in November [2017], we sanctioned an ... IRGC-QF[] network involved in a large-scale scheme to counterfeit Yemeni bank notes to support its destabilizing activities. This network employed deceptive measures to circumvent European export control restrictions ....

In addition to Iran's financing of terrorism ..., the IRGC has an extensive presence in Iran's economy, including in the energy, construction, mining, and defense sectors. *In our engagements both here in the United States and abroad, we have made clear that companies doing business in Iran face substantial risks of transacting with the IRGC or IRGC-linked entities.*

*This risk is heightened by the lack of transparency in the Iranian economy, which is one of the least transparent in the world. Indeed, Iran is on the FATF's blacklist precisely because it has failed to address such systemic deficiencies in its controls to combat terrorist financing ....* This has led the FATF to highlight for the past decade the terrorist financing risk emanating from Iran and the threat that it poses to the international financial system. Thus far, Iran has failed to fulfill its commitments to the FATF in addressing its weak controls.

We will continue to take action to protect the international financial system and to combat Iran's relentless campaign to support terrorism. (Emphasis added.)

337. Zhao, moreover, was personally responsible for causing Binance's deliberate indifference to giving FTOs widespread access to the Binance exchange. In his plea agreement with the DOJ, Zhao agreed that "[s]tarting at least as early as August 2017 and continuing to at least October 2022, [he] violated the Bank Secrecy Act . . . by willfully causing [Binance] to fail to implement and maintain an effective [anti-money laundering] program."

338. If there were any doubt about Defendants' willful blindness, admissions from Binance employees put them to rest. As noted *supra*, Binance's Money Laundering Reporting Officer reacted to a statement from the compliance officer in 2020 lamenting that Binance was facilitating criminal transactions by saying, "we see the bad, but we close 2 eyes." That is a textbook admission of willful blindness from a senior employee in the relevant department.

**VI. Defendants Knowingly And Substantially Assisted Terrorist Attacks Committed By The IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS That Targeted The United States And Killed Or Injured Plaintiffs**

339. Defendants’ decision to knowingly enable terrorist groups to transact on the Binance exchange provided those groups substantial benefits. Defendants gave uniquely dangerous actors (FTOs) access to a uniquely dangerous product (cryptocurrency) on a uniquely dangerous platform (Binance’s exchange)—which these terrorists used to finance attacks.

340. Money is the lifeblood of terrorism. As senior Treasury official Daniel Glaser testified before Congress in June 2016:

[O]ur efforts to combat terrorist financing [depend on] ... [d]isrupting the flow of funds to terrorists and terrorist organizations[,] [which] has become an integral part of our broader strategy to combat terrorism. While not a silver bullet, these efforts stem from the recognition that by employing financial tools, we can degrade the functioning of terrorist organizations and make it harder for them to accomplish their destructive goals. While the financial cost of carrying out an individual terrorist attack can be quite low, recruiting, training and sustaining operatives, procuring weapons, and developing the infrastructure necessary to support these activities requires generating and moving substantial funds, often between distant locations.

341. As detailed in voluminous warnings from the U.S. government, U.N., blockchain analysis firms, terrorism scholars, and NGOs, cryptocurrency provided a laundry list of benefits for terrorist organizations and state sponsors of terrorism. Terrorist groups embraced cryptocurrency as a tool for fundraising, performing rapid cross-border transfers to other members of the organization, training and transporting operatives, cybercrime, sanctions evasion, extortion, and buying and selling goods, including illegal weapons and drugs.

342. When Defendants deliberately flowed through millions of dollars in cryptocurrency and fiat currency each year to the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS, Defendants supplied such FTOs with the funds needed to pay for every link in the terrorist attack kill chain: recruiting, training, arming new fighters, securing logistics

and communications support, financing martyr payments and disability payments to incentivize terrorism, making post-attack bounty payments to reward attacks that resulted in a dead American, purchasing American hostages taken by other groups, and buying non-public attack-related intelligence on a target.

343. By knowingly and willfully giving the world's most notorious anti-American FTOs access to Binance's global cryptocurrency exchange, Defendants gave these groups access to the international financial community. Defendants' actions enabled the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS to access and transact freely on a global cryptocurrency exchange. This was a force multiplier for these FTOs and their (illicit) use of cryptocurrency—which they used to fund terrorist attacks. Defendants' culpable actions provided unusually potent, cross-cutting lethal aid to the IRGC's, Hezbollah's, Kataib Hezbollah's, Hamas's, PIJ's, al-Qaeda's, and ISIS's attacks targeting the United States, including Plaintiffs, for at least eight reasons.

344. *First*, Defendants' combination of the Binance exchange and cryptocurrency supplied **global reach and unrivaled ease of transferring funds across international borders** to Defendants' IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS customers, which amplified the killing power of such FTOs—especially when one of the parties to the transaction (like the FTOs here) resided in Iraq, Iran, Syria, Lebanon, Gaza, Afghanistan, Pakistan, Kenya, or Niger, and the other party resided in the United States or another country with robust AML/CFT rules and regulations. These FTOs use cryptocurrencies for transactions, including on the dark web, such as purchasing weapons and other illicit goods for terrorist

attacks. As Stephanie Dobitsch, Deputy Under Secretary, Office of Intelligence and Analysis at Homeland Security, explained during her testimony to Congress in July 2021:

As we have learned in our fight against terrorism, terrorists are highly adaptive and have proven successful in exploiting new and emerging technologies to plan attacks against U.S. interests and the homeland. While some of those technologies, such as drones and 3D printing, pose direct harm, it is often access to sources of funding that are difficult to trace or attribute that ***allow terrorist groups even greater means to conduct a broad range of operations against the United States***. Additionally, as governments and the global financial industry devote more resources to restricting terrorist use of traditional banking systems, ***the relative ease and anonymity of cryptocurrencies are helping to offset these restrictions***, including for other malicious actors seeking to do harm to the United States. Since at least 2015, we have observed terrorists experimenting with cryptocurrencies to ***obfuscate their financial activities, procure materials, and solicit donations for their operations***. These activities have spanned the spectrum of terrorist ideologies—from Racially or Ethnically Motivated Violent Extremists (RMVEs), to groups like the Islamic State of Iraq and ash-Sham (ISIS), al-Qaeda, and HAMAS. Using cryptocurrencies may be attractive to terrorists and supporters of violent extremism because they appear to offer a level of anonymity and less government oversight. We have seen ISIS supporters around the world requesting donations in cryptocurrency. . . . Also, receiving payments through cryptocurrency has risen in popularity.<sup>9</sup> (Emphasis added.)

345. Further, as terrorism scholar Jessica Davis observed in 2021: “Moving money is a fundamental component of terrorist financing. More often than not, terrorists want to raise money in one location, store funds in another, and use the money in yet another. . . . The ability to move funds is critical for terrorist organizations, cells, and individuals because funds often need to flow from groups to cells, among groups, and from donors to organizations.” Likewise, as Treasury reported in the *2024 National Terrorist Financing Risk Assessment*, with respect to terrorist groups like Hizballah, the IRGC-QF, Hamas, and ISIS:

Terrorist groups may also use virtual assets to transfer funds to other members or related groups using VASPs or peer-to-peer virtual asset transfers . . . that do not involve a regulated financial institution. . . . While some of the VASPs used by terrorist groups may be local to their operations, in particular for exchanging

---

<sup>9</sup> “Operation” and “Operations” refer to terrorist attacks. The U.S. government, United Nations, U.K., E.U., and terrorism scholars agree and follow the same nomenclature.

virtual assets for fiat currency, they can also leverage VASPs based all over the world to send and receive virtual assets. Regardless of whether terrorist groups received funds from donations or transfers from other groups, they will likely require VASPs to exchange virtual assets for fiat currency, which is often necessary to purchase goods and services.

346. *Second*, Defendants’ combination of the Binance exchange and cryptocurrency supplied **encryption and anonymity** to Binance’s IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS customers, which strengthened the attacks of the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS. As Treasury reported in the *2024 National Terrorist Financing Risk Assessment*, for example, terrorist groups like Hizballah, the IRGC-QF, Hamas, and ISIS foreseeably “could use anonymity-enhancing technologies such as anonymity-enhanced virtual assets and techniques, like virtual asset mixing, to obfuscate the source, destination, or movement of virtual assets” “to finance their operations,” *i.e.*, attacks targeting the United States.

347. National security and terrorist-financing scholars and NGOs have reached similar conclusions: in 2021, for example, Eric Lorber, of the Foundation for Defense of Democracies, testified before Congress: “Terrorist organizations and rogue regimes have likewise used different types of cryptocurrency to evade U.S. sanctions and finance their activities.

. . . [C]ertain cryptocurrencies provide a degree of anonymity that can be exploited by terrorist organizations and rogue regimes.”

348. *Third*, the Binance exchange and cryptocurrency combined to provide a **secure, digital, and ready store of value** for the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS (as to their respective holdings) that could be converted into fiat currency (like U.S. dollars) as needed. Accordingly, Defendants’ operation of the Binance exchange allowed terrorists to do all these things pseudonymously and—thanks to willfully unscrupulous actors

like Defendants—without being subject to AML/CFT rules and oversight from responsible financial institutions. Defendants’ scheme to grant the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS access to cryptocurrency through Defendants’ illegal operation of the Binance exchange sustained and strengthened such FTOs, enabling more attacks that targeted the United States and Americans, including Plaintiffs. For example, as Treasury reported in the *2024 National Terrorist Financing Risk Assessment*:

[M]ost cases of terrorists using virtual assets involve groups fundraising online and specifically soliciting virtual assets from donors. Such fundraising campaigns are often disseminated through social media or encrypted apps ... and often solicit funds in virtual assets and fiat currency, enabling the donor to decide which method to use. Individual donors can send virtual assets from a VASP or an unhosted virtual asset wallet to a virtual asset address owned by the terrorist group. Groups may use the funds for a range of purposes, including the procurement of weapons, propaganda creation or dissemination, logistics, or planning a specific act of violence, although purchasing goods and services often requires exchanging virtual assets for fiat currency.

349. In other words, the Binance exchange was a safe space for terrorists to securely deposit the proceeds from their illegal activity (*e.g.*, theft, extortion, human trafficking and drug trafficking), which they could then transfer to affiliates worldwide as needed for use in terrorist attacks.

350. *Fourth*, the Binance exchange and cryptocurrency **transaction speed** made Defendants’ assistance an especially potent source of terrorist finance for the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS. For example, as terrorism scholar Jessica Davis explained in 2021: “In recent years, two emerging trends have had significant interplay for terrorist financing financial technologies (including cryptocurrency) and social media. Terrorist financiers use social media to solicit donations and then use financial technologies including cryptocurrency to transfer the funds internationally. These fund-raising campaigns are easy to set

up, can reach hundreds or thousands of people almost instantaneously, and enable funds to be transferred within minutes or hours.”

351. This feature of Defendants’ assistance uniquely incentivized attacks because it made it easier for the terrorists’ financial sponsors—who were often social media fans of the terrorists who felt compelled to donate to the FTOs after being persuaded by social media calls to do so—because Defendants’ illegal operation of the Binance exchange made it easy for such FTOs’ donors around the world to rapidly pay financial rewards to terrorists after successful attacks. As terrorism scholar Martin Gallagher explained in his 2024 book *Terror For Profit*, using IRGC-trained Hamas as an example:

The diaspora tentacles and reach of Gaza Strip-origin terrorist groups stretch less than those of Hezbollah. ... Hamas ... [used] weapons ... to deadly effect. It had also been at the forefront of cryptocurrency and, until October 7th, saw a spike in currency flow after every successful attack it mounted. (Cleaned up.)

352. *Fifth*, Defendants provided a **backdoor to the U.S. financial system** through their business strategy to operate their illegal cryptocurrency exchange in the United States (including New York), while willfully violating U.S. AML/CFT rules and regulations, U.S. sanctions, and U.S. reporting requirements. Defendants even communicated such points to their VIP customers as a market differentiator. Defendants’ deliberate actions enabled supporters of the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS who resided in the United States to confidently route their financial donations to such FTOs from the United States to places like Iran and Syria and to persons like the terrorists in those FTOs without having to: (a) navigate a complex, paper-trail creating, bank transfer; (b) worry about whether the

transaction would get blocked by a bank officer following AML/CFT rules; or (c) expose the communication to potential investigative or intelligence intercepts.

353. U.S. government reports confirmed the foregoing. In May 2022, for example, Treasury reported to Congress, in the *National Strategy for Combating Terrorist and Other Illicit Financing*, that “the key threat[] .... findings” with respect to “Terrorist Financing Threats” included that “U.S.-based supporters of foreign terrorist groups continue[d] to send relatively small sums (ranging from several hundred to tens of thousands of dollars) to facilitators outside of the United States working on behalf of these groups” because one of the “ways” that some “terrorists move[d] funds raised in the United States” occurred when “terrorist groups and their supporters ha[d] used, or [were] seeking to use, virtual assets.” Likewise, as Treasury reported to Congress in the *2024 National Terrorist Financing Risk Assessment*:

[C]ontributions from individual supporters also supplement [ISIS]’s cash flows. ISIS has sought to aggressively fundraise online using social media . . . and virtual asset service providers (VASPs) for fund transfers. ISIS facilitators have adapted to new technologies like virtual assets. For example, certain branches, such as ISIS-K, have increased their understanding of virtual assets. ISIS also seeks to raise money to free pro-ISIS sympathizers and potential ISIS recruits, including children, from camps and prisons throughout Syria. Some fundraising networks generated funds for this specific purpose in ... the United States, and elsewhere, which were then transferred via hawala networks to ... ISIS ... in Syria. ...

ISIS-related activity in the United States is largely relegated to lone, self-radicalized individuals seeking to ... [*inter alia*] offer financial support to the group. Financial activity linked to ISIS in the United States typically involves supporters collecting or sending small amounts of money abroad or financing their own or others’ travel to ISIS conflict zones. This money generally comes from legal means, often personal savings, and sometimes may be collected on behalf of others. Individuals may coordinate the donations through encrypted mobile applications like Telegram [and] send the funds in the form of virtual assets .... Some U.S. persons have also engaged in more extensive financial and fundraising activity on behalf of ISIS.

354. *Sixth*, the Binance exchange and cryptocurrency’s **ability to work on mobile phone networks in conflict zones**—including, *inter alia*, Iraq, Syria, Lebanon, Gaza,

Afghanistan, Pakistan, Kenya, and Niger—made the Binance exchange/cryptocurrency combination a uniquely lethal source of terrorist finance for the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS. As Treasury reported in the *2024 National Terrorist Financing Risk Assessment*, for example, “virtual assets” were “used across the globe (especially in areas with poor financial and telecommunications infrastructures)” by “[t]errorist groups” like the “Qods Force,” “Hizballah,” “Hamas,” and “ISIS” in order “to finance their operations,” *i.e.*, attacks targeting the United States.

355. *Seventh*, Defendants’ operation of Binance’s illegal exchange served as a **currency “off-ramp”** that encouraged Binance’s IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS terrorist customers to convert cryptocurrency to fiat currency (*e.g.*, U.S. dollars) for use in the mainstream economy without New York and U.S. AML/CFT regulation or oversight. Indeed, throughout the Relevant Period, the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS sought out access U.S. dollars because the dollar was stable, widely accepted, and could be used to purchase weapons and other supplies to commit terrorist attacks. For example, as Chainalysis explained in 2020: “fiat off-ramp services like exchanges are crucial for money laundering, as those are the services where criminals can turn crypto into cash, which is likely their ultimate goal. Fiat off-ramps[’]. . . compliance teams have an important role to play in flagging incoming illicit funds and preventing them from being exchanged for cash.” Similarly, as Jeremy Sheridan, Assistant Director of the Office of Investigations with the U.S. Secret Service, testified before Congress in July 2021:

For crypto-currencies or other digital assets to be utilized within the mainstream economy—namely, to exchange them for most goods or services—they usually must be converted into government-backed fiat currency, such as the U.S. dollar .... This conversion typically occurs through ‘exchanges,’ money services businesses which allow for the purchase and sale of digital assets with fiat currency. Exchanges, both as on-ramps and off-ramps to the cryptocurrency

economy, have been a particularly effective data source and control point for governments to focus their efforts”—but “terrorist groups persistently seek to avoid U.S. and foreign AML and KYC requirements by utilizing exchanges that do not adhere to [U.S.] laws or reporting requirements.

By knowingly providing terrorist groups an unregulated off-ramp to convert cryptocurrency into fiat currency—which those groups could use to buy weapons, supplies, or otherwise support attacks—Defendants provided enduring, valuable, and covert aid to the attacks targeting the United States that were committed by Binance’s FTO customers.

356. *Eighth*, the Binance exchange also provided terrorists a **closed ecosystem**—largely free from public and regulatory oversight—for conducting transactions with other Binance users. That is because transactions between Binance users were recorded only on Binance’s internal, private ledger; those transactions were not recorded on public blockchains. In other words, there was no public record of transactions occurring exclusively between Binance users. This means that if an ISIS terrorist in Iraq sent a Bitcoin from his Binance account to the Binance account of an ISIS terrorist in Syria, there would be no public record of that transaction; there would only be a private record, memorialized on Binance’s internal ledger.

357. As terrorism scholar Jessica Davis observed in 2021, the ability to transact globally, while obscuring the details of their transactions, enables terrorist attacks and frustrates counterterrorism efforts:

The financial entities provide access to the international financial system, cover stories for the terrorists’ money movement, accept false names and documentation, and a variety of other benefits. ...

Terrorist groups, cells, and individuals all use varying levels of financial tradecraft to obscure the sources, destinations, and uses of their funds. They use [*inter alia*] ... financial technologies, cryptocurrencies, and specialized financial facilitators. ... [T]errorist actors’ use of financial tradecraft is a critical element of their financing methods and can, with little effort, complicate counterterrorism practitioners’ efforts to follow the money trail.

358. Decades of official U.S. government reports warned and confirmed that FTOs depended on funding—including through digital currencies—to finance every aspect of their lethal attacks targeting the United States. In April 2008, for example, U.S. Special Operations Command published *Disrupting Threat Finances: Using Financial Information To Disrupt Terrorist Organizations*, which observed, *inter alia*:

- a. “‘There are two things a brother must always have for jihad, himself and money.’ - Al Qaeda Operative”
- b. “[I]nternational terrorist groups need significant amounts of money to organize, recruit, train, and equip new adherents and to otherwise support their infrastructure. Terrorist organizations must have financing to pay for protection (such as safe havens), to bribe corrupt public officials, for recruiting, for indoctrination and training, for general operational expenses and equipment, to provide logistical support, to communicate, to increase their organizations infrastructure, to support operatives’ families, to provide support to families of martyrs, to fund humanitarian efforts, and for various other sundry items. In short, terrorist organizations require considerable amounts of funds to be raised, moved, and stored through various means to conduct operations.”
- c. “Since [9/11], detecting and preventing terrorist activities have been top priorities for the United States Government (USG). One of the goals of President George W. Bush’s Global War on Terrorism (GWOT) is to deny terrorist groups access to the international financial system, to impair their ability to raise funds, and to expose, isolate, and incapacitate their financial networks. Like most organizations, terrorist groups need financing to organize, recruit, train, and equip adherents.”
- d. “Terrorist organizations appear to be migrating toward [] alternative financing mechanisms such as ... digital currency[,] ... [which] [a] close examination of terrorist networks reveals ... [was among the] key nodes in their organizations that have become the preferred conduits used by terrorists to fund and facilitate attacks. If, therefore, the world is serious about disrupting the terrorists’ operating environment, countries need to look at key nodes in the network, such as financing, which terrorist’s organizations use to raise, launder, and transfer funds. ... Terrorist organizations raise funds through a variety of sources, including ... individual contributors, witting and unwitting; criminal activity; corporate contributors, witting and unwitting; operating businesses; state sponsors; and legal employment. These funds provide the interchangeable, easily transportable means to secure all other forms of material support. Once the funds are raised, terrorist organizations move the funds through several mechanisms, including ... digital currency .... If the U.S. and its partners are going to succeed in the fight against terrorists, they must deprive terrorists of the material support they require by disrupting and monitoring the various funding sources and by interdicting the different movement mechanisms currently available.”

- e. “Based on the fact that terrorist organizations require financing to operate, finances are a critical factor, and disrupting finances will contribute to the U.S., its allies, and partner nations’ success in the fight against terrorism.”

359. In January 2020, likewise, Treasury publicly warned in its *National Strategy for Combating Terrorist and Other Illicit Financing* report to Congress that a wide array of jihadist FTOs like al-Qaeda used “unlicensed money transmitters” and “digital assets” to finance attacks:

In the aftermath of the 9/11 attacks, U.S. authorities targeted the financial vulnerabilities, *such as the ... unlicensed money transmitters*, that allowed Al-Qaida to move money around the world and into the United States to fund the attacks. ... U.S. authorities have identified U.S.-based individuals who raise and send money to support violence overseas .... [Some] terrorist groups ... are more regularly seeking small dollar donations in digital assets. ...

U.S. authorities are closely monitoring *terrorist use of digital assets*. ... [T]errorist organizations and their supporters and sympathizers are constantly looking for new ways to raise and transfer funds. As there is a growing acceptance of digital assets in society, it is likely that terrorist organizations will also leverage digital assets to move funds. According to U.S. law enforcement, some terrorist organizations are growing more comfortable with seeking small dollar donations in digital assets. (Emphasis added.)

360. The U.N. reached the same conclusion. In 2021, for example, the U.N. Security Council repeatedly warned that FTOs in Syria—where the IRGC, Hezbollah, Kataib Hezbollah, al-Qaeda, and ISIS all had a large presence—were intensifying their use of cryptocurrencies to finance attacks by, *inter alia*, paying terrorist operatives and funding “bounty” payments offered for successful attacks targeting the United States:

- a. “The reported use of cryptocurrency in the Syrian Arab Republic has increased in recent months. There are ongoing reports of terrorist fighters or their family members seeking to raise funds via cryptocurrency wallet addresses.”
- b. “Member States remain concerned about the use of the Internet and social media by terrorists to raise and move funds. A number of States have announced law enforcement actions targeting the financing of terrorism through cryptocurrencies.”

361. The significance of Defendants’ transaction amounts was especially pronounced when viewed in light of the low marginal cost of the IRGC’s, Hezbollah’s, Kataib Hezbollah’s, Hamas’s, PIJ’s, al-Qaeda’s, the Taliban’s, and ISIS’s individual attacks.<sup>10</sup>

362. Accordingly, Defendants’ deliberate provision of the ability to raise and transfer *even small amounts* of cryptocurrency to such FTOs had outsized effects on the terrorists’ ability to commit deadly attacks. As Treasury Under Secretary Mandelker noted in 2019 during the cryptocurrency industry’s *CoinDesk Consensus* conference, “the cost of carrying out a terrorist attack can be low,” as a “radicalized suicide bomber can bring a tragic end to the lives of hundreds for nothing more than the price of duct tape, a vest, and supplies”—as such, the industry “cannot afford to allow any money to flow to terrorists.”

363. CipherTrace, in reports targeted at the cryptocurrency industry, similarly warned about the low cost of carrying out a terrorist attack. Quoting Jason Blazakis, former director of the Finance and Designations Office at the State Department’s Bureau of Counterterrorism, and then-director of the Center on Terrorism, Extremism, and Counterterrorism, CipherTrace reported that “[t]errorists don’t have to raise a lot of crypto or cash to maintain sanctuary for sleeper cells or, worse yet, the ammunition, guns, and bombs that can maim innocent civilians.” Indeed, per CipherTrace, Blazakis warned that “[w]hile a thousand dollars may not seem like a lot of money, in the hands of the wrong person, it can do all of the above and much more.”

364. Indeed, terror attacks are inexpensive, and small numbers of terrorists can wreak havoc. For example, Hamas attacks typically fit this pattern. As Dr. Matthew Levitt observed in his 2007 book, *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*:

---

<sup>10</sup> Given their shared pedigrees, common geographies, and similar (often identical) tactics, techniques, and procedures, the rough cost per attack was generally the same between these groups in their respective geographies.

[In] a 2002 interview, Salah Shehada, the founder of [ Hamas's ] Izz al-Din al-Qassam Brigades, claimed an operation could cost from \$3,500 to \$50,000. A Hezbollah member has put the figure of a terror attack at \$665-\$1,105 .... Another terrorist from Palestinian Islamic Jihad, Ahmad Sari Hussein, received \$2,210 ... for his terrorist activity, while Wael Ghanam, a Tanzim activist from the Tulkarem refugee camp, said he received \$7,000 to manufacture explosive charges. Others have claimed that a suicide bombing mission could be set up for as little as \$150, consisting essentially of a bomb of chemicals (sugar or fertilizer), a battery, a light switch, wire, and a belt. Still others figure the cost of each bomb belt at \$1,500 to \$4,300.

365. Studies consistently confirmed that the cost of nearly all attacks in by terrorist groups in the Middle East in the post-9/11 era ranged from around \$2,000 per attack to around \$20,000 per attack—with most on the low end of that spectrum. IEDs, for example, usually cost around \$100 per bomb. Generally, Hamas and Hezbollah fighters were paid around \$200 per month, while leaders were paid around \$400. Indeed, al-Qaeda bragged in online publications in the early 2010s that it could conduct a sophisticated, transnational bombing targeting Americans for less than \$5,000. As terrorism scholars Jessica Stern and J. M. Berger explained in 2016:

Asymmetrical warfare is defined by asymmetry. Any terrorist ideology that can attract five recruits and the contents of their checking accounts can make headlines for months. *A terrorist group with twenty willing recruits and half a million dollars can make headlines for years.* (Emphasis added.)

366. At those rates, even a single transaction that flowed \$5,000 to an IRGC proxy or ISIS would have financed substantial terrorist violence. At the time, a \$5,000 payment would have put 10 terrorists (at \$200 per fighter) and two commanders (at \$400 per commander) in the field for a month, equipped with about 20 IEDs. Or terrorists could have spent the \$5,000 to purchase dozens of bomb components or to finance multiple complex attacks. The transactions Defendants enabled were orders of magnitude higher—and they materially strengthened the terrorists' ability to commit the attacks that killed and injured Plaintiffs.

367. U.S. government studies confirmed the dramatic impact of even marginal financial contributions to FTOs operating in the Middle East. For example, one DoD study of

AQI—which followed a substantially similar approach as every FTO here when it came to attack logistics—found a statistically significant relationship between small-dollar contributions and terrorist attacks, concluding that each successful terror attack in Iraq required on average only \$2,732 to execute. The study thus demonstrated that even marginal reductions in the terrorist funds flowing to an AQI-like FTO corresponded with a statistically significant reduction in terrorist violence. The converse was also true. For every \$2,700 (or its rough equivalent) Defendants gave to FTOs like AQI (including every FTO here) successors, they financed roughly one new terrorist attack. As a result, the millions in dollars in value that Defendants flowed to the FTOs here was more than enough to fund thousands of attacks—sufficient to kill every Plaintiff in this case multiple times over.

368. This effect was linear. Simply put, more money equaled more terrorist attacks. As Dr. Margaret Sankey of the U.S. Naval Institute and Air University, concluded in 2022:

With the caveat and reminder that operations don't cost a large amount in proportion to sustainment, VNSAs [Violent Non-State Actors] whose budgets have been reduced have to make hard decisions about maintaining their capabilities. In some cases, there's a clear pattern that more money means more attacks, with al-Qaeda in Iraq consistently increasing by one attack for every \$2,700 sent by the central leadership to sectors. Mustafa Abu al-Yazid, an al-Qaeda financing chief, put it starkly: "There are hundreds wishing to carry out martyrdom-seeking operations, but they can't find the funds to equip themselves. So funding is the mainstay of jihad."

369. Defendants' admissions, public reporting, and blockchain analysis confirm that Defendants knowingly and substantially assisted several FTOs by enabling them and their affiliates to transact on the Binance exchange.

370. The below allegations reflect the transactions of which Plaintiffs are aware. These allegations reflect what Plaintiffs have been able to piece together without discovery. The full details of the volume of transactions performed by FTOs on the Binance.com exchange, and the

full scope of Defendants’ knowledge of those transactions, rest in Defendants’ sole control. On information and belief, discovery will show substantially more transactions on the Binance exchange occurring contemporaneously with the attacks in this case—causing even more value to flow through to the FTOs who committed the attacks.

**A. The IRGC’s, Hezbollah’s, and Kataib Hezbollah’s Attacks on Plaintiffs**

**1. Defendants Knowingly Enabled IRGC Members, Affiliates, and Fronts to Transact on the Binance Exchange**

371. Defendants knowingly enabled IRGC members, affiliates, and fronts to transact on the Binance exchange.

372. As explained, at its founding Binance deliberately avoided taking any measures to prevent users in sanctioned jurisdictions, including Iran, from accessing its platform. It was not until mid-2018 that Binance gestured toward implementing a compliance program—but even then, Binance’s efforts to keep users from sanctioned jurisdictions off its platform were deliberately “implemented inadequately, at least in part due to Binance senior management’s decisions to appear compliant while disregarding known sanctions risks.”

373. As OFAC’s investigation revealed, “[n]umerous communications between Binance leadership demonstrate that Binance’s failure to implement effective controls was the product of *deliberate choices* by senior management that effectively ensured Binance’s sanctions compliance program would primarily remain only a ‘*paper program*.’” (Emphasis added.)

374. As the below “internal discussions” make clear, Binance and Zhao’s noncompliance with U.S. sanctions on Iran was intentional and brazen:

- a. “On August 3, 2018, Binance’s then CCO explained in a chat message to a Binance employee that ‘our stance is [n]ot to openly do business with Iran due to sanctions. [I]t affects our banking relationships. I understand that we still support [I]ranian customers but that has to be done non-openly.’”

- b. “The following month, in a September 2018 response to an inquiry from the then Deputy Head of Compliance asking if Binance was servicing users from Iran on Binance.com, the then CCO explained that, with respect to users from sanctioned countries, ‘[w]e are servicing [them] but non-public.’ He further added, ‘[I] [t]old [yo]u we have [I]ranian customers; [the CEO of Binance] knows also. And allows it.’”
- c. “The then CCO would go on to explain to the Deputy that sanctions restrictions in Binance’s Terms of Use ‘has to be there to protect us, [it is] protective language. In biz, ceo doesn’t want to enforce.’ Later, in the same chat, Binance’s then Deputy Head of Compliance stated that Binance’s Operations Director said that Binance ‘can service sanctioned countries’ on Binance.com.”
- d. “In another September 2018 message, the then Deputy Head of Compliance explained to the then CCO that ‘[the CEO] keeps saying that compliance is here to make Binance APPEAR compliant.’ (Emphasis in original.)”
- e. “In an October 18, 2018 message regarding the potential blocking of sanctioned country Internet Protocol (IP) addresses, the then CCO informed Binance’s Chief Executive Officer (CEO) that ‘we currently have users from sanction[ed] countries on [Binance.com],’ adding that the ‘[d]ownside risk is if fincen or ofac has concrete evidence we have sanction[ed] users, they might try to investigate or blow it up big on worldstage.’”
- f. “In June 2019, the CEO demonstrated his own broad awareness of U.S. sanctions prohibitions applicable to Binance when he told a senior Binance employee that ‘the U.S. has this law: you have to prevent Americans and any terrorists from doing any transactions. In order [for America] to accomplish this, if you serve Americans or service American sanctioned countries, you have to give your data to the American regulators.’ He added, ‘the U.S. says we are not focusing on the dollar; if our citizens use your services we can arrest/catch you.’”

375. Further, in or around June 2018, Binance’s Chief Compliance Officer deliberately “misled a financial institution by writing in a Due Diligence Anti-Money Laundering Compliance form that ‘we use IP blocking to deny business from sanctioned countries. It is also clearly written in our Terms and Conditions that we prohibit business with all sanctioned countries.’” Per OFAC, Binance’s statements “misrepresented Binance’s actual compliance procedures and communicated a commitment and practices that did not in fact exist.”

376. Additionally, Binance’s willfully deficient geofencing controls—controls that would have allowed it to prevent access from users in sanctioned jurisdictions—are additional powerful evidence of Defendants’ intentional violation of U.S. sanctions on Iran. As FinCEN explained, “Binance’s policies, procedures, and internal controls around the location of its customers were critically deficient, as reflected by its geofencing controls. Binance’s geofencing . . . allowed users from high-risk jurisdictions to access the platform without appropriate controls. Binance personnel were aware that its poor geofencing controls meant that users from jurisdictions designated by [FATF] on the grey or blacklist or subject to comprehensive sanctions could access the platform; this also meant that Binance’s AML controls would not be sufficient to meet its SAR obligations.”

377. Another example: “in April 2020, a company with which Binance wanted to partner expressed concern that, ‘as part of the due diligence process, [our] Compliance team was able to open accounts with an . . . Iranian address on Binance.com. The Iranian test was opened using an Iranian IP and an Iranian address.’ This was *far from an isolated incident*.” (Emphasis added.)

378. As *Reuters* reported in 2022, Binance’s “popularity in Iran was known inside the company. Senior employees *knew of, and joked about*, the exchange’s growing ranks of Iranian users, according to 10 messages they sent to one another in 2019 and 2020. . . . ‘IRAN BOYS,’ one of them wrote in response to data showing the popularity of Binance on Instagram in Iran.” (Emphasis added.)

379. Binance *actively encouraged* users from sanctioned countries, including Iran, to transact on its exchange. According to OFAC, “Binance senior management” “encouraged the use of VPNs and surreptitiously allowed U.S. users and sanctioned jurisdiction users to trade

even after ostensibly blocking them. For example, Binance continued to allow trades by users who were logged in from an IP address in a comprehensively sanctioned jurisdiction so long as that user had submitted KYC documents from a non-sanctioned jurisdiction.” As reported by *Reuters* in 2022, “Binance itself had supported the use of VPNs. Zhao . . . tweeted in June 2019 that VPNs were ‘a necessity, not optional.’”

380. Binance and Zhao were at all times more interested in “feigning compliance rather than addressing the company’s actual risk,” as “reflected in the intentionally weak implementation of its controls” to prevent users in sanctioned jurisdictions, including Iran, from transacting on the exchange, according to that *Reuters* investigation.

381. Defendants’ actions caused a staggering volume of transactions involving Iranian actors—including transactions by IRGC members, affiliates, and fronts—to be processed through the Binance exchange.

382. By Binance’s “own estimates, between June 2017 and September 2021, Binance processed over 1,000,000 transactions with an aggregate value *in excess of \$500 million* between U.S. users and users accessing the platform via an Iranian IP address.” (Emphasis added.) This includes “a significant volume of direct transactions with various Iranian [cryptocurrency] exchanges.”

383. Moreover, as FinCEN identified and Defendants admitted, Binance knowingly processed:

several transactions with [convertible virtual currency] wallets associated with ***sanctioned entities and individuals***, including: (i) EnExchanger, an Iranian entity designated for assisting the cyber actors behind the SamSam ransomware attacks; and (ii) Ahmad Khatibi Aghada, an individual associated with the sanctioned ***Iranian Revolutionary Guard Corps*** (IRGC) that engaged in ransomware activities. Binance failed to file SARs with FinCEN on any of these transactions, ***even after OFAC’s designations***. Binance was ***similarly aware*** of other Iran-related illicit transactions that occurred on the Binance.com platform but filed no SARs with FinCEN. For example,

prior to the institution of full KYC, IranVisaCart, and other illicit actors maintained accounts with Binance, taking advantage of Binance’s policies surrounding opening multiple accounts with weak or no KYC. Binance was made aware of these accounts and the related illicit transactions *as early as 2019*, and *filed no SARs* with FinCEN. (Emphasis added.)

384. Defendants’ admissions in guilty pleas and settlements with the U.S. government reflect only a small fraction of overall Iran-based traffic that flowed through Binance. That is because the U.S. government focused on those transactions where a U.S. user’s trade was matched internally with an Iranian user’s trades. Accordingly, transactions that involved individuals in Iran, including those affiliated with the IRGC, that did not also involve U.S. users were not included in the transaction volume. Thus, the true volume of illicit transactions involving Iranian actors is much higher.

385. In November 2022, *Reuters* thoroughly investigated and reported on the volume of Iran-affiliated transactions occurring on the Binance exchange. The *Reuters* investigation found that, since between 2018 and November 2022, Binance “processed Iranian transactions *with a value of \$8 billion*.” (Emphasis added.) “Almost all the funds, *some \$7.8 billion*, flowed between Binance and Iran’s largest crypto exchange, Nobitex, according to a review of data from leading U.S. blockchain researcher Chainalysis.” (Emphasis added.)

386. *Reuters* found in that investigation that, notwithstanding Binance’s “announce[ment] that customers would no longer be able to open accounts and use its services without identification,” Binance “processed almost \$1.05 billion in trades directly from Nobitex and other Iranian exchanges, according to the Chainalysis data.”

387. Plaintiffs’ analysis of publicly available blockchain data, moreover, confirms that from 2018 to 2022, Binance processed roughly *\$8 billion* in transactions for the following Iranian cryptocurrency exchanges: Nobitex, CoinNik Market, Rabex, Sarmayex, and Wallex. In

addition to those transactions, blockchain analysis shows that funds have *continued* to flow between Nobitex and the Binance.com exchange as recently as September 2024.

388. Indeed, Plaintiffs’ preliminary analysis of open-source intelligence and publicly available information, including blockchain ledgers, confirms that Defendants knew that IRGC fighters, financiers, and supporters used the Binance exchange to support the IRGC’s terrorist objectives. Based on Plaintiffs’ analysis, Defendants knew that from 2017 to 2024 Binance helped the IRGC obtain at least **\$1.3 million** through transfers involving identified IRGC addresses that flowed through Binance, involving 4 distinct wallet addresses.<sup>11</sup> This estimate is conservative, and the correct number is likely much higher, in light of the constraints described below—many of which result from Binance’s deliberate choices in how it structured its exchange.

389. Plaintiffs’ preliminary estimate of transactions by IRGC-owned or -affiliated wallets is based on publicly available wallet attribution data. Sources for wallet attribution include: (1) U.S. sanctions on specific wallet addresses terrorist-owned or -affiliated wallets, which are included on OFAC’s Specially Designated Nationals and Blocked Persons List (“SDN List”); (2) terrorist-owned or -affiliated wallet addresses included on Anti-Semitism and Other (“ASO”) lists published by Israel’s National Bureau for Counter Terror Financing (“NBCTF”);<sup>12</sup> (3) legal filings, including forfeiture proceedings pursued by the U.S. government, that identified

---

<sup>11</sup> All values set forth in connection with Plaintiffs’ transaction estimates are based on the approximate value, in USD, of the particular cryptocurrencies transferred, at the time of such transaction.

<sup>12</sup> NBCTF is the Israeli authority that consolidates, coordinates, and outlines Israel’s national-level enforcement policy in the country’s fight against terrorist groups and their financial networks. It was established as part of the Israel Ministry of Defense in March 2018, and is globally recognized as a reliable authority on, and global leader in, combatting terrorism and the financial infrastructure that supports it—particularly as to terror groups’ rapid adoption of cryptocurrency and blockchain technologies over the last 5-7 years.

terrorist-owned or -affiliated wallet addresses; (4) open-source intelligence sources; and (5) industry-standard blockchain analysis techniques used by AML/CFT and compliance functions at cryptocurrency exchanges and blockchain analysis firms, such as clustering analyses.

390. The same information that Plaintiffs used as the basis for their estimate was available to, and known to, Defendants throughout the Relevant Period. On information and belief, throughout the Relevant Period, Defendants closely monitored wallet attributions contained in the sanctions designations and legal filings that Plaintiffs relied on for their preliminary estimate of transactions. This is because—in addition to having a team of employees purportedly focused on compliance and risk monitoring internally—Binance had contractual relationships with several blockchain analysis firms, whose tools Binance used for AML/CFT monitoring on its platform. Those blockchain analysis firms incorporated wallet addresses that had been formally sanctioned or designated by the U.S. or Israeli government into their AML/CFT monitoring software. Those firms’ tools thus alerted Defendants in real-time, or close to it, whenever a sanctioned or otherwise high-risk wallet address sought to transact on the Binance exchange. *See supra* Part V(C).

391. Beyond these official designations, these blockchain analysis firms themselves flagged wallets as operated by or affiliated with terrorist groups, such as the IRGC, based on their own diligence. Binance had contractual relationships with several blockchain analysis firms, whose tools Defendants used for AML/CFT monitoring on its platform. *See supra* Part V(C). Those firms provided Defendants a constant stream of warnings regarding wallets that were likely connected to terrorist groups—but Defendants willfully disregarded those warnings

and permitted wallets labeled as connected to the IRGC to transact on the Binance exchange.<sup>13</sup>

Accordingly, Defendants knew, or were at least aware of the substantial risk, that the wallets included in Plaintiffs' analyses were operated by or affiliated with the IRGC long *before* they were formally designated as such and/or rendered subject to Israeli and/or U.S. government sanctions.

392. The above estimate is based on those IRGC transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants' knowledge of, and support for, the IRGC's transactions on the Binance exchange rest within Defendants' sole control. In part, this is because, as discussed, data about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is *not* available on public blockchains. That information is available only to Binance, memorialized on Binance's internal, nonpublic ledgers. Further, on information and belief, Binance's private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying data about the devices used to perform the transactions—that confirm additional IRGC-related transactions occurred on the Binance exchange.<sup>14</sup> Discovery into Binance's internal records will thus likely uncover many other

---

<sup>13</sup> On information and belief, those blockchain analysis firms' labels were accurate, based on what they represented to be robust screening and diligence practices.

<sup>14</sup> As Binance explained at least as early as its 2018 privacy policy for users: "When you use Binance platform services, Binance automatically receives and records information received from your browser and computer, including but not limited to your IP address, browser type, use of language, access date and time, software and hardware features, and other data." On information and belief, Binance collected such information about its users, or similar user information, throughout the Relevant Period whenever users transacted on the Binance exchange or other Binance platforms.

similar transactions and/or ways in which Defendants knowingly and substantially assisted the IRGC.

393. Under binding IRGC orders, those profits were necessarily spent financing IRGC operations. On June 8, 2003, the Iranian regime published an official directive ordering the IRGC to dedicate the profits it earned from its commercial fronts to its core mission, i.e., protecting and exporting the Islamic Revolution through acts of terrorism (“Logistics Policy Directive”). The Logistics Policy Directive provided that with respect to the profits derived from whenever “any unit” of “the Islamic Revolutionary Guard Corps ... and related organizations ... sign[ed] contract agreements for civil projects,” “[t]he monies received from any [such IRGC-related] contract...shall be deposited to the Chancery, and its equivalent shall be placed at authority of the [IRGC] from the credit determined in the annual budget, so that it would be used for the costs related to the [IRGC-related] contract, also the strengthening of the [IRGC], and replacing [IRGC] equipment and machinery parts” needed for its operations, i.e., terrorism. Moreover, under the Directive, the IRGC “can, proportionally to [the IRGC’s] needs, exchange or sell excess material, and equipment and machinery” to finance IRGC operations.

394. At bottom, the Logistics Policy Directive established—and was known to establish—an ironclad rule: the IRGC was authorized and encouraged to act as contractors in development schemes, subject to the requirement that any profit would be used to help the IRGC “purchase and upgrade equipment for the Revolutionary Guards and fund its other activities,” i.e., the IRGC’s central Anti-American terrorist mission under Iran’s constitution. As a result, IRGC profits were required under Iranian law to be reinvested in the IRGC’s specific lanes of activity that supported terrorism. The Logistics Policy Directive, in effect, mandated that IRGC profits derived from IRGC fronts be used primarily to enable IRGC-sponsored terrorism by

providing off-the-books funding sources for key IRGC weapons programs—the entire point of the Logistics Policy Directive in the first place.

395. From June 2003 through present, the Logistics Policy Directive was always in force, always required that such IRGC profits be dedicated to sponsoring acts of terrorism, and was always published in Iran’s Official Gazette.

396. Defendants knew about the Logistics Policy Directive because they were familiar with basic Iranian government pronouncements as part of their country-related diligence, and because media reports beginning in 2003 alerted Defendants to such fact because such reports regularly described the Directive as a potential IRGC-related compliance challenge for companies contemplating partnerships with IRGC-controlled entities. In October 2007, for example, Ali Alfoneh, of the American Enterprise Institute, publicly warned about the Logistics Policy Directive, which he explained was intended to help the IRGC “purchase and upgrade equipment for the Revolutionary Guards and fund its other activities,” *i.e.*, IRGC-sponsored acts of terrorism targeting the United States.

397. In May 2010, similarly, Iranian expat media outlet *Peyk-e Iran* publicly warned (as translated from Farsi by Plaintiffs) that “the IRGC ... gradually expanded its power and influence since 1979” through fronts “reflecting [the] Iranian economy’s dominance by a military-mafia institution,” for which “the Logistics Directive” served “as a component of this expansion” because the Directive was an “order that all IRGC units ... must participate in civil projects as contractors,” upon which the IRGC relied to assert the “IRGC’s dominance in security ... institutions, and IRGC companies’ influence in [the] telecom industry” through “IRGC-controlled companies” that owned stakes in communications firms.

398. In 2015, likewise, IRGC scholar Hesam Forozan publicly warned that the Logistics Policy Directive:

appease[d] the [IRGC] ... [as an official] decree summoning units designated and identified by the Islamic Revolution's Guards Corps... and its affiliated institutions to act as contractors in development schemes and projects. Any profit, the directive continued, should be transferred to the Chancery, which in turn would fund not only the [IRGC] contract in question, but would use any surplus to purchase and upgrade equipment for the Revolutionary Guards and fund its other activities.

399. Moreover, Defendants disregarded regular U.S. warnings that conduct like theirs could finance IRGC-sponsored attacks by Hezbollah, Kataib Hezbollah, Hamas, PIJ, and the Taliban. On February 17, 2018, for example, Lieutenant General H.R. McMaster (U.S. Army, ret.), then-U.S. National Security Advisor, addressed the Munich Security Conference in Munich, Germany, which was one of the most widely covered intergovernmental events of 2018. Before an in-person audience comprised of hundreds of senior executives from a wide array of banks, companies, law firms, and consulting firms, LTG McMaster confirmed in sum and substance that multinational financial firms—like Binance—that consciously chose to engage in substantial transactions with unknown Iranian counterparties likely enabled terrorist attacks, directly warning that even plain vanilla cross-border transactions between such multinational entities and their Iranian customer counterparts funded IRGC-sponsored terrorist attacks throughout the Middle East. LTG McMaster warned, *inter alia*:

- a. “Jihadist terrorist organizations continue to use the mass murder of innocents as their principal tactic in their evil war against all civilized people.”
- b. “Iran’s destabilizing activities[] includ[e] its development and proliferation of missiles and its support for terrorist proxies ... across the Greater Middle East. The Iranian regime foments this violence with support from commercial entities affiliated with the Islamic Revolutionary Guards Corps .... As a matter of international security, and moral conscience, we must stop doing business with IRGC-affiliated interests ....”
- c. “Hezbollah is a designated terrorist organization, ... [a]nd, in terms of Iran’s role, I think what you see now is what Hezbollah really is: ... a proxy of the Iranians. And [] they

have been ... receiving more and more missile and rocket capabilities and improving those capabilities to threaten Israel and ... the whole region.”

- d. “[T]ake a step back and [] see what Iran is actually doing in the region ...[:] applying the Hezbollah model to the Greater Middle East, in which they want weak governments in power ... that are dependent on Iran for support while they grow terrorist organizations ... that are outside of that government’s control that can be turned against that government if that government acts against Iranian interests. ... We see this in Iraq ... [a]nd what’s particularly concerning is that this network of proxies is becoming more and more capable as Iran seeds more, and more capable, ... more destructive, weapons into these networks.”
- e. “[W]hen you look at the biggest investors in Iran[:] ... *When you invest in Iran, you’re investing in the IRGC. You might as well cut the Islamic Revolutionary Guards Corps a check and say, ‘please use this to commit more murder across the Greater Middle East.’* So when we look at the biggest trading partners with Iran, of course we see Russia, China, but we also see Japan, South Korea, and Germany in the top three, and I think *it’s time for all of us to focus our business intelligence efforts to figure out who we are really doing business with and let’s do everything we can to cut off funding to the Islamic Revolutionary Guards Corps.*” (Emphasis added.)

From February 17, 2018 onward, media outlets in the U.S., Europe, and Asia widely reported LTG McMaster’s specific warning about IRGC business underlined above.

400. Defendants also willfully disregarded real-time warnings from iconic American firms known for their commitment to compliance. In August 2017, for example, iconic American company Apple Inc. removed Iranian “apps” from Apple’s iOS App Store and publicly stated: “Under US sanctions regulations, the App Store cannot host, distribute, or do business with, apps or developers connected to certain US embargoed countries.” As Defendants knew, such rationale applied with even greater force to Binance’s activities given that Binance had even greater U.S. regulatory burdens than did Apple. Freedom House, an NGO, reported in 2020 that “[s]ince the United States has increased diplomatic pressure on Iran under President Donald Trump, many companies such as the software development platform GitHub no longer offer services to Iranians, forcing them to use domestic alternatives. Samsung and the Apple Store have also restricted services to Iranians due to US sanctions. Some Bitcoin sites have also been

removed citing US sanctions. . . . [m]any international tech companies have closed their services to Iranian users.”

## 2. Defendants’ Actions Enabled the IRGC’s and Its Proxies’ Terrorist Attacks

401. By knowingly and willfully processing voluminous transactions by Iranian actors—including sanctioned IRGC members and other entities associated with the IRGC—Defendants culpably enabled the IRGC to support and commit terrorist attacks.

### a. Defendants Helped the IRGC Fund Terrorist Attacks Using Revenue from Large-Scale Cryptocurrency Mining Operations

402. On information and belief, Defendants knew that during the Relevant Period, Iran and the IRGC embraced cryptocurrency mining (or “cryptomining”) as a strategy to raise revenue for terrorist attacks and otherwise evade U.S. sanctions.

403. By way of background, cryptomining is the process by which powerful, decentralized computers are used to verify cryptocurrency transactions and generate new cryptocurrency coins. When a transaction is made between wallets, the addresses and amount are entered into a block on the blockchain. The block is assigned some information, and all the data in the block is put through a cryptographic algorithm (called hashing)—processed by cryptocurrency miners. In return for their efforts, the miners are rewarded with cryptocurrency—both from transaction fees as well as the minting of new Bitcoins.

404. Indeed, in 2021, Iran was estimated to mine as much as seven percent of the global Bitcoin market—making it one of the top eight Bitcoin-producing nations worldwide. One estimate indicates that Iran’s Bitcoin mining produced as much as ***\$1 billion in revenue*** in 2021.

405. The revenue generated from cryptomining benefitted the IRGC’s terrorist agenda: the revenue generated from cryptomining has enabled the IRGC “to purchase imports, move

funds domestically and internationally, and fund Hamas and other terrorist organizations,” as explained by Senators Elizabeth Warren and Angus King.

406. This is because the IRGC controls—and directly benefits from—Iran’s cryptomining operations. Indeed, as Iran scholar and professor Shahram Kholdi explained during testimony during a 2024 session of the Canadian House of Commons, “[s]ince 2015 the IRGC has . . . has been very active in the dark web, cryptocurrency transactions and other international money-laundering operations.”

407. Throughout the Relevant Period, public reports—including many in the cryptopress—corroborated the IRGC’s control over Iran’s cryptomining operations. As reported by Iranian journalist Ehsan Nowrozi, writing in *The Independent (Persian)* in July 2019:

Bitcoin’s bubble cycle . . . over a few weeks in the last three months of 2017 dazzled the world’s eyes. It was during these days that ***the “IRGC” octopus, which has dominated all profitable economic areas in Iran, began serious investments in this field*** by changing the use of abandoned sheds to advanced bitcoin mining sheds.

Take a look at this list. This is the official list of individuals, places, and institutions that are exempt from paying electricity bills: “Mosques, husseiniyas, Quranic institutions, Dar al-Quran, seminaries, martyrs’ flower gardens, shrines, houses of scholars, villages, religious minorities, veterans over 25 percent, and families of martyrs.”

This means that the IRGC mafia can take butter from running water. The cost of mining each bitcoin is not so low for any person or entity in the world. By imposing police policies, they prevent the official entry of mining equipment into Iran and import unlimited amount of mining equipment from their unofficial docks behind the scenes.

In addition, the IRGC has the ability to suppress all domestic rivals, petty competitors who are hiding somewhere in the basements of mosques and schools, or this bankrupt poultry farm and ranch. Upon discovering these petty rivals, the IRGC confiscates their equipment and adds the same equipment to its extensive mining network.<sup>15</sup> (Emphasis added.)

---

<sup>15</sup> Translated by Plaintiffs using Microsoft Edge Browser (emphasis added).

408. Citing this 2019 article, *CoinDesk* reported that “Iranian journalist Ehsan Norouzi wrote in 2019 that the list of entities running mining operations on free electricity might actually be much bigger: the country’s elite armed forces, the Islamic Revolutionary Guard Corps, control a broad network of religious schools, mosques and other entities that get electricity for free.” *CoinDesk* also noted the centrality of the regime to Iran’s mining operations. Chinese cryptomining businesses that established a foothold in Iran attributed their success to having “good relations with the Ministry of Energy, the Ministry of Foreign Affairs and even the army in Iran.” Indeed, “Iran clearly sees crypto mining as a way to generate income for the state.”

409. Indeed, taking advantage of its control over Iran’s customs and imports, the IRGC has confiscated tens of thousands of cryptomining rigs. As reported on *Bitcoin.com* in 2019, “Iran has been gathering interest from bitcoin miners due to the country’s super cheap electricity,” but entering the market “has proven easier said than done.” That is because “there are harsh import regulations and the *Islamic Revolutionary Guard Corps are still detaining or confiscating machines* at border points.” (Emphasis added.) According to a miner who established a cryptomining in Iran, the Iranian government ““added this energy-hungry device (bitcoin miner) to the list of 2,000 banned shipments to come in.”” By 2019, the IRGC had reportedly ““confiscated *at least 40,000 crypto mining rigs* of varied models.”” (Emphasis added.)

410. Iran scholar Barabara Slavin, director of the Future of Iran Initiative and a non-resident senior fellow at the Atlantic Council, similarly commented in 2022 that cryptomining is ““more a regime phenomenon than something used by ordinary people,”” with the IRGC ““behind these . . . mining efforts.””

411. The IRGC benefitted financially from cryptomining in at least two ways. First, IRGC-affiliated cryptomining operations receive transaction fees in exchange for mining cryptocurrency (*i.e.*, verifying a transaction). Second, the IRGC benefits because “Iranian cryptominers are required to sell the crypto they produce to the Iranian central bank,” and the Central Bank of Iran funnels money to the IRGC and its terrorist proxies, including Hamas and PIJ. Cryptomining thus provides the IRGC the funds to finance its and its proxies’ attacks.

412. Defendants culpably enabled the IRGC to profit handsomely from these extensive cryptomining efforts. *First*, Binance’s lax KYC procedures and willingness to allow Iranian entities access to its cryptocurrency platform provided Iranian cryptominers an enormous, constant supply of transactions to verify. By offering Iranian miners access and the ability to verify transactions for trades on the Binance exchange, Defendants’ actions helped enable the rapid expansion of Iran’s cryptomining industry. *Second*, by willfully providing the IRGC access to the Binance exchange, Defendants supercharged the IRGC’s cryptomining efforts. Namely, Defendants ensured that cryptocurrency generated from the IRGC’s mining operations could be used to transact globally, with little oversight. The IRGC could use cryptocurrency generated from its mining operations in Iran to transact through Binance. This enabled the IRGC to convert Iranian-mined cryptocurrency into other types of cryptocurrencies or fiat currencies (such as U.S. dollars), which it could use to purchase goods and services for its terrorist attacks; or transfer Iranian-mined cryptocurrency to terrorist proxies in Syria, Iraq, or Israel. Without access to a global cryptocurrency exchange like Binance, the IRGC’s ability to use its cryptocurrency mining operations, profit from them, and transfer such profits to Hezbollah, Kataib Hezbollah, Hamas, PIJ, and al-Qaeda to finance such FTOs’ attacks, would be greatly inhibited.

**b. Defendants' Actions Enabled the IRGC to Profit from Ransomware Operations That Funded Terrorist Attacks**

413. Defendants enabled the IRGC to profit, and otherwise benefit, from ransomware operations. As an example, Binance admitted that wallets associated with “EnExchanger, an Iranian entity designated for assisting the cyber actors behind the SamSam ransomware attacks” transacted on the Binance exchange.

414. Indeed, Plaintiffs’ detailed analysis of open-source intelligence and publicly available information, including blockchain ledgers, confirms that Iranian actors associated with EnExchanger and the SamSam ransomware attack, including Mohammad Ghorbaniyan, transacted on the Binance exchange.

415. As explained in connection with OFAC’s designation, Ghorbaniyan “helped exchange digital currency (bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims.” His actions “enabled Iranian cyber actors to profit from extorting digital ransom payments from their victims,” and were “[c]entral to the SamSam ransomware scheme’s success,” as he “helped the cyber actors exchange digital currency derived from ransom payments into Iranian rial and also deposited the rial into Iranian banks.”

416. The SamSam ransomware scheme was authorized by, and benefitted, the IRGC. It was widely understood that the IRGC used offensive cyber operations as an extension of foreign policy. And, based on the sophistication of the SamSam ransomware scheme, it is highly likely the perpetrators were IRGC agents. Ghorbaniyan himself was a seasoned actor with deep ties to Iran’s national security establishment, including personal ties to the IRGC. The SamSam scheme, moreover, funneled money at least \$6 million in payments into Iranian banks—a sector controlled by the IRGC, *see supra* Part I(A)(3)(b).

**c. Defendants' Actions Enabled the IRGC to Efficiently Fund Its and Its Proxies' Terrorist Attacks**

417. Defendants' willful processing of Iranian cryptocurrency transactions was a boon for the IRGC and for its ability to attack Americans. As summarized by Senator Elizabeth Warren during a 2023 congressional hearing: "***The biggest crypto mine in [Iran] is run by the Islamic Revolutionary Guard Corps,***" and "***Binance has processed \$8 billion worth of Iranian transactions since 2018.***" (Emphasis added.) Defendants have thus knowingly allowed the "Islamic Revolutionary Guard Corps [to] use[] crypto mining to replace revenue that they lose through sanctions." That, according to Lieutenant General Scott Berrier, Director of the Defense Intelligence Agency, "certainly threatens our US forces in the region" because "***[c]ryptocurrency, Bitcoin is one method of how [the IRGC] finance[s] their [] operations.***" (Emphasis added.)

418. Indeed, the Israeli government seized cryptocurrency wallets linked to the IRGC-QF and its primary terrorist proxy, Hezbollah, in summer 2023. As reported in the *Times of Israel* in June 2023,

Defense Minister Yoav Gallant on Tuesday revealed that Israel has seized digital wallets linked to Iran's Islamic Revolutionary Guard Corps' Quds Force and the Iran-backed Hezbollah terror group, confiscating millions of dollars in cryptocurrency. . . . "This is the first incident of this magnitude, in which an infrastructure led by Hezbollah and the Iranian Quds Force that transferred millions of dollars to be used by terror elements was thwarted," Gallant said. He added that since the beginning of the year, members of Hezbollah, the IRGC's Quds Force, and "Syrian elements" have used cryptocurrency to fund their daily activities. The funding comes from a third party, and is handed over to the terror groups via money exchangers, Gallant said.

419. Not only does the IRGC exploit cryptocurrency to enrich itself and fund terrorist proxies, the IRGC transfers cryptocurrency to terrorist proxies, including Hamas and PIJ.

420. As Treasury Deputy Secretary Adewale O. Adeyemo explained before Congress in May 2024, "over the past year, we have seen the Islamic Revolutionary Guard Corps-Qods

Force (IRGC-QF) transfer cryptocurrency to Hamas and the Palestinian Islamic Jihad (PIJ) in Gaza.” Other U.S. law enforcement officials have similarly confirmed that the “IRGC has provided Hamas, among other things . . . tens of millions of dollars in annual funding for Hamas’s terror wing, including through cryptocurrency payments.”

421. For example, as reported in the *Wall Street Journal* in 2023, “[a]round 2020, crypto became a method of large-scale transfers between Iran and the group [Hamas] within the hawala networks, according to the current and former Israeli officials and ex-U.S. officials. Since then, crypto has been ‘an essential part for their operational activity,’ one senior [National Bureau for Counter Terror Financing of Israel] official said. Iran has long been Hamas’s primary benefactor, with the U.S. putting regular funding from Tehran at roughly \$100 million a year.” Cryptocurrency was a way for Iran to “lessen the risks of moving physical money and goods.” By using cryptocurrency, “Hamas and affiliates such as Palestinian Islamic Jihad to receive large sums from Iran during the two years that preceded the attacks on Israel” in October 2023.

422. Senators Elizabeth Warren and Angus King explained in 2024 that “[t]he Iranian military has used crypto to fund known terrorist groups like Hezbollah” and, they predict, “will continue to use crypto” to fund their proxies’ terrorist attacks.

423. Cryptocurrency transfers involving the IRGC and its proxies occurred on the Binance exchange. Indeed, Plaintiffs’ blockchain analysis shows that Binance hosted at least one wallet held by Lebanon-based Syrian money exchanger Tawfiq Muhammad Sa’id al-Law, who moved over **\$11.9 million** in 130 different cryptocurrency transfers through the Binance exchange over the course of 2023. According to Treasury, al-Law “provided Hizballah with digital wallets to receive funds from IRGC-QF commodity sales,” and “similarly conducted cryptocurrency transfers for sanctioned Hizballah officials.” Indeed, after sanctioning al-Law’s

wallets in May 2023 for al-Law’s connections to terrorist groups, the Israeli government later seized cryptocurrency wallets controlled by al-Law on the grounds that al-Law’s “terrorist infrastructure belonging to Hezbollah and the Iranian Quds Force . . . operated to transfer funds through digital currencies for Quds Force and Hezbollah.” Blockchain analytics platform Chainalysis similarly reported that “Al-Law . . . worked with senior Hezbollah operators like Muhammad Qasim Al-Bazzal and Muhammad Ja’far Qasir — both of whom are sanctioned by OFAC — to operate Hezbollah’s crypto funding infrastructure. Qasir in particular is a critical conduit for financial disbursements from Iran’s Quds Force used to fund Hezbollah’s activities.”

424. After NBTCF added a wallet controlled by al-Law on a sanctions list in May 2023 based on his Hezbollah ties and designated the wallets of 28 intermediaries that had engaged in heavy transaction volume with the al-Law wallet, Binance *continued to allow* 19 of those listed wallets to transact on and with the Binance exchange to the tune of *more than \$53 million* for his work with Hezbollah and other FTOs. Nearly half of these transfers occurred three weeks or more after those wallets were listed. Because these intermediary wallets were designated and had direct transfers with the wallet of a known terrorist financier, Binance knew or was willfully blind to the likelihood that those wallets were engaged in terrorism finance-related activity.

425. The IRGC, moreover, has used cryptocurrency to pay agents to conduct assassinations and kidnapping. Time and again, evidence from foiled IRGC plots has revealed the IRGC’s preference to use cryptocurrency to make cross-border payments to agents, including IRGC agents hired to conduct kidnappings and/or assassinations in the United States.

**B. Hamas's and PIJ's Attacks on Plaintiffs**

426. Defendants knew that Hamas and PIJ terrorists and supporters transacted on the Binance exchange.

427. Binance admitted in its settlement with FinCEN that it was told repeatedly that Hamas terrorists were using the Binance exchange, including in February 2019.

428. As Binance admitted, in April 2019, “Binance received reports from its third-party service provider . . . identifying Hamas-associated transactions” on the Binance exchange. Despite those reports, Binance filed no SARs with FinCEN. “Instead, Binance’s former Chief Compliance Officer attempted to influence how its third-party service provider reported on Binance’s conduct.”<sup>16</sup>

429. Defendants also admitted that in July 2020, “after a third-party service provider flagged accounts associated with ISIS and Hamas, the former Chief Compliance Officer described it as ‘[e]xtremely dangerous for our company’ and instructed compliance personnel to ‘[c]heck if he is a VIP account, if yes, to... [o]ffboard the user but let him take his funds and leave. Tell him that third party compliance tools flagged him.’” Following its consistent practice of concealing criminal and terrorist activity on its exchange, “Binance failed to file a SAR on transactions related to an individual designated by OFAC for support of a terrorist group. The individual was allowed to keep an account for several years in withdrawal-only status after designation and withdraw their balance.”

---

<sup>16</sup> Defendants’ knowledge that Hamas was using the Binance exchange necessarily would have alerted Defendants that it was highly likely that the IRGC, Hezbollah, PIJ, and Kataib Hezbollah were also using the Binance exchange due to those groups’ shared finance networks. Moreover, that same notice of Hamas’s use of the Binance exchange would have alerted Defendants that it was highly likely that ISIS was using the Binance exchange, as ISIS’s financial tradecraft was similar to Hamas’s.

430. Beyond these direct admissions that Defendants knew about Hamas terrorists using the Binance exchange, Defendants received a multitude of other, contemporaneous warnings that Hamas terrorists used, or were attempting to use, mainstream cryptocurrency exchanges, like Binance.

431. In a widely publicized 2019 episode, Hamas published a video where it urged supporters to contribute to the group through cryptocurrency. In that video, Hamas instructed its supporters to create an account on a mainstream exchange—including Binance—to use for cryptocurrency donations.

432. A screenshot from that 2019 video<sup>17</sup> shows ***Binance’s logo*** in connection with the instruction to Hamas supporters to “[c]reate a new account” on Binance is reproduced below (red box added):



433. Plaintiffs’ preliminary analysis of open-source intelligence and publicly available information, including public blockchain ledgers, confirms that Defendants knowingly processed

<sup>17</sup> This screenshot is from a version of the since-disabled Hamas webpage (“fund.alqassam.ps”) that was archived as an Internet Archive webpage capture on June 6, 2019, available at <https://web.archive.org/web/20190606050636/http://fund.alqassam.ps/>.

transactions on the Binance exchange for Hamas fighters, financiers, and supporters to support Hamas's terrorist attacks, throughout the Relevant Period.<sup>18</sup> Based on Plaintiffs' analysis, Defendants knew that from 2017 to 2024 Binance helped Hamas obtain at least **\$56 million** through transfers involving identified Hamas addresses that flowed through Binance. Defendants also knowingly processed several millions of dollars' worth of cryptocurrency transactions with, and transfers to and from, Hamas-owned or linked wallets on the Binance platform even after those wallets were **formally** sanctioned based on those wallets' ownership by or strong connections with Hamas terrorists. Plaintiffs' estimate is conservative, and the correct number is likely much higher, in light of the constraints described below—many of which result from Binance's deliberate choices in how it structured its exchange.

434. The above estimate is based on those Hamas transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants' knowledge of, and support for, Hamas's transactions on the Binance exchange rest within Defendants' sole control. In part, this is because, as discussed, information about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is **not** available on public blockchains. That data is available only to Binance, memorialized on Binance's internal, nonpublic ledgers. Further, on information and belief, Binance's private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying information about the devices used to perform the transactions—that confirm additional Hamas-related transactions occurred on the Binance

---

<sup>18</sup> Plaintiffs' approach to blockchain analysis is explained *supra* ¶¶ 389-391.

exchange. Discovery into Binance’s internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted Hamas.

435. Further, with respect to PIJ, FinCEN determined (and Defendants admitted) that Binance knowingly processed transactions for dozens of users with “tens of millions of dollars in transactions with an identified PIJ network.”

436. Plaintiffs’ preliminary analysis of open-source intelligence and publicly available information, including public blockchain ledgers, confirms that Defendants knowingly processed transactions on the Binance exchange for PIJ fighters, financiers, and supporters to support PIJ’s terrorist attacks, throughout the Relevant Period.<sup>19</sup>

437. Plaintiffs’ preliminary estimate confirms that Defendants knew that PIJ fighters, financiers, and supporters used the Binance exchange to support PIJ’s terrorist attacks. Based on Plaintiffs’ analysis, Defendants knew that from 2017 to 2024 Binance helped PIJ obtain at least **\$59 million** through transfers involving identified PIJ addresses that flowed through Binance. This estimate is conservative, and the correct number is likely much higher, in light of the constraints described below—many of which result from Binance’s deliberate choices in how it structured its exchange

438. The above estimate is based on those PIJ transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants’ knowledge of, and support for, PIJ’s transactions on the Binance exchange rest within Defendants’ sole control. In part, this is because, as discussed, information about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users)

---

<sup>19</sup> Plaintiffs’ approach to blockchain analysis is explained *supra* ¶¶ 389-391.

is *not* available on public blockchains. That information is available only to Binance, memorialized on Binance’s internal, nonpublic ledgers. Further, on information and belief, Binance’s private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying information about the devices used to perform the transactions—that confirm additional PIJ-related transactions occurred on the Binance exchange. Discovery into Binance’s internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted PIJ.

439. Reports throughout the Relevant Period corroborate Hamas’s and PIJ’s use of cryptocurrency and cryptocurrency exchanges to raise funds and commit terrorist attacks. In addition to the many warnings discussed above, *supra* Part IV, additional examples follow.

440. As the cryptopress media outlet *CoinDesk* reported in early 2020, “the Israeli International Institute for Counter-Terrorism (ICT) found the al-Nasser Brigades . . . used bitcoin sent from overseas as a means of funding operations in and out of the Gaza Strip. . . . [T]he group – which the Jerusalem Post says has links to Hamas – used bitcoin to avoid sanctions, offer a degree of anonymity to donors from overseas and enable cross-border money transfers.”

441. As *CoinDesk* reported in 2021, “Israeli officials have moved to seize potentially millions of dollars in cryptocurrency from addresses it says are controlled by Hamas. The wallets, 84 in all, hold a mix of cryptocurrencies . . . according to files from the [Israeli] National Bureau for Counter Terrorist Financing. Tracing firm Elliptic estimated in a blog post that the crypto wallets have received over \$7.7 million in total.” Chainalysis similarly reported that “Israel’s [NBCTF] released information on the seizure of cryptocurrency held by several wallets associated with donation campaigns carried out by Hamas. The seizure included but was not

limited to . . . Hamas’s military wing. This action comes after a sizable uptick in cryptocurrency donations to Hamas in May following increased fighting between the group and Israeli forces.”

442. In September 2021, Coinbase—a direct competitor of Binance—published an “overview of the use of cryptocurrencies in terrorist financing” where it found that, among terrorist groups, “Hamas has raised the most funds . . . . [I]kely because Hamas actively solicits donations primarily in the form of [Bitcoin] on their website and related Telegram channels.” According to Coinbase, “Hamas’s fundraising efforts are staggering” and “appear to correlate to the time frames of the most intense geopolitical conflict.”

443. The *Wall Street Journal* reported in October 2023 that in the years leading to the October 7 terrorist attacks in Israel, “three militant groups—Hamas, Palestinian Islamic Jihad and their Lebanese ally Hezbollah—received large amounts of funds through crypto, according to a review of Israeli government seizure orders and blockchain analytics reports. Digital-currency wallets that Israeli authorities linked to the PIJ received as much as \$93 million in crypto between August 2021 and June [2023], analysis by leading crypto researcher Elliptic showed. . . . Wallets connected to Hamas received about \$41 million over a similar time period, according to research by another crypto analytics and software firm, Tel Aviv-based BitOK.”

444. Further, as TRM Labs reported in 2024, “TRM research found a growing interest in and use of crypto by terrorist groups and their supporters to solicit donations and conduct cross-border payments. This includes . . . Iranian-backed groups like Hamas and Palestinian Islamic Jihad (PIJ), which have received hundreds of thousands of dollars’ in cryptocurrency over the past few years.”

445. Treasury, moreover, warned in the 2024 *National Terrorist Financing Risk Assessment* that “Hamas facilitators have used numerous methods to collect and transfer funds

into the Gaza Strip. These include crowdfunding websites and sham charities, where in some cases, the destination of the funds was concealed under the guise of humanitarian efforts. In other cases, they solicited funds directly for their cause from sympathetic donors. Hamas has also used complicit VASPs and money transmitters throughout the globe to move funds. In the aftermath of the October 7, 2023, terrorist attacks, Treasury designated a Gaza-based VASP called Buy Cash Money and Money Transfer Company for serving as a key node in Hamas's virtual asset fundraising schemes. The same entity has also been identified as being involved with funds transfers on behalf of other terrorist groups." Treasury cautioned that "Hamas is a well-resourced group that garners substantial financial resources from numerous and diverse sources" and is "prolific in soliciting donations . . . in both fiat and virtual assets."

446. And, as the United States has explained in a recent criminal complaint filed against Hamas leaders, "Hamas raises money to fund its terrorist activities through a variety of methods, including by soliciting and receiving cryptocurrency payments, advertising the ostensible anonymity of such transactions. Since 2019, Hamas's military wing has used social media and other platforms to call for cryptocurrency contributions from supporters abroad, including in the United States, to Hamas-controlled virtual wallets, explicitly acknowledging that those payments would be used to fund Hamas's campaign of violence. Through these mechanisms, Hamas has received tens of millions of dollars in cryptocurrency payments to fund its activities." Indeed, in that criminal complaint, the United States provided a detailed history about how Hamas has "solicited and received funding to promote [its] terrorist activities through a variety of illicit means, including cryptocurrency payments, advertising the ostensible anonymity of such transactions."

447. It is highly probable that a substantial percentage of Hamas's and PIJ's cryptocurrency transactions during the Relevant Period moved through the Binance exchange because, among other reasons, it was the largest exchange by transaction volume that willfully (and completely) disregarded enforcing AML/CFT and KYC requirements during that time.

448. Hamas and PIJ also benefitted from Defendants' choice to knowingly allow IRGC members, affiliates, and fronts to transact on the Binance exchange. As explained, Defendants culpably enabled the IRGC to profit from its access to the Binance exchange, which enabled the IRGC to flow value through to its terrorist proxies, including Hamas and PIJ.

### **C. Al-Qaeda's Attacks on Plaintiffs**

449. Defendants knew that al-Qaeda terrorists and supporters transacted on the Binance exchange.

450. In Binance's settlement with FinCEN, FinCEN found (and Defendants admitted) that "Binance user addresses were found to interact with bitcoin wallets associated with . . . Al Qaeda," and "no SARs were filed with FinCEN." Indeed, FinCEN "observed more than 200 direct bitcoin transactions, in the aggregate worth several hundred thousand dollars, with Al-Qaeda-associated" wallets during the Relevant Period.

451. Defendants knowingly processed transactions for cryptocurrency wallets associated with al-Qaeda. Defendants had contractual relationships with several blockchain analysis firms, whose tools Defendants used for AML/CFT monitoring on its platform. *See supra* Part V(C). Those blockchain analysis firms provided Defendants a constant stream of warnings regarding wallets that were likely connected to al-Qaeda (even though Defendants willfully disregarded those warnings). On information and belief, those blockchain analysis firms' labels were accurate, based on what they represented to be robust screening and diligence practices.

452. Indeed, Plaintiffs’ preliminary analysis of open-source intelligence and publicly available information, including blockchain ledgers, confirms that Defendants knew that Al-Qaeda fighters, financiers, and supporters used the Binance exchange to fund al-Qaeda attacks.<sup>20</sup> Based on Plaintiffs’ analysis, Defendants knew that from 2017 to 2024 Binance helped al-Qaeda obtain at least **\$1.8 million** through transfers involving identified al-Qaeda addresses that flowed through Binance, involving 90 distinct wallet addresses. This estimate is conservative, and the correct number is likely much higher, in light of the constraints described below—many of which result from Binance’s deliberate choices in how it structured its exchange.

453. The above estimate is based on those al-Qaeda transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants’ knowledge of, and support for, al-Qaeda’s transactions on the Binance exchange rest within Defendants’ sole control. In part, this is because, as discussed, information about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is **not** available on public blockchains. That data is available only to Binance, memorialized on Binance’s internal, nonpublic ledgers. Further, on information and belief, Binance’s private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying information about the devices used to perform the transactions—that confirm additional al-Qaeda-related transactions occurred on the Binance exchange. Discovery into Binance’s internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted al-Qaeda.

---

<sup>20</sup> Plaintiffs’ approach to blockchain analysis is explained *supra* ¶¶ 389-391.

454. Public reporting corroborates al-Qaeda’s use of cryptocurrency to raise funds and commit terrorist attacks. *See supra* Part IV.

455. It is highly probable that a substantial percentage of al-Qaeda’s cryptocurrency transactions during the Relevant Period moved through the Binance exchange because, among other reasons, it was the largest exchange by transaction volume that willfully (and completely) disregarded enforcing AML/CFT and KYC requirements during that time.

456. Al-Qaeda also benefitted from Defendants’ choice to knowingly allow IRGC members, affiliates, and fronts to transact on the Binance exchange. As explained, *supra*, Defendants culpably enabled the IRGC to profit from its access to the Binance exchange, which enabled the IRGC to flow value through to al-Qaeda.

#### **D. ISIS’s Attacks on Plaintiffs**

457. Defendants knowingly processed transactions for ISIS terrorists and supporters.

458. Binance admitted in its settlement with FinCEN that it knew that ISIS terrorists were transacting on the Binance exchange. *See, e.g., supra* ¶ 310. FinCEN, moreover, “observed multiple direct transactions between Binance and ISIS-associated [convertible virtual currency] wallets” between July 2017 and July 2023.

459. Binance knew about cryptocurrency wallets associated with ISIS that transacted on its platform. Defendants had contractual relationships with several blockchain analysis firms, whose tools Defendants used for AML/CFT monitoring on its platform. *See supra* Part V(C). Those blockchain analysis firms provided Defendants a constant stream of warnings regarding wallets that were likely connected to ISIS (even though, as discussed *see supra* Part V(C), Defendants willfully disregarded those warnings). On information and belief, those blockchain analysis firms’ labels were accurate, based on what they represented to be robust screening and diligence practices.

460. Indeed, Plaintiffs’ preliminary analysis of open-source intelligence and publicly available information, including blockchain ledgers, confirms that Defendants knew that ISIS fighters, financiers, and supporters used the Binance exchange to support ISIS’s terrorist objectives.<sup>21</sup> Based on Plaintiffs’ analysis, Defendants knew that from 2017 to 2024 Binance helped ISIS obtain at least **\$2.9 million** through transfers involving identified ISIS addresses that flowed through Binance, involving 27 distinct wallet addresses. This estimate is conservative, and the correct number is likely much higher, in light of the constraints described below—many of which result from Binance’s deliberate choices in how it structured its exchange.

461. The above estimate is based on those ISIS transactions of which Plaintiffs are aware that Defendants knowingly processed on the Binance platform. This list is not exhaustive; it reflects what Plaintiffs have been able to piece together without discovery. The full details of Defendants’ knowledge of, and support for, ISIS’s transactions on the Binance exchange rest within Defendants’ sole control. In part, this is because, as discussed, information about transactions that occur solely on the Binance exchange (*i.e.*, transactions among Binance users) is **not** available on public blockchains. That information is available only to Binance, memorialized on Binance’s internal, nonpublic ledgers. Further, on information and belief, Binance’s private transaction data includes granular transaction details—such as the geographic location of users involved in the transactions and identifying information about the devices used to perform the transactions—that confirm additional ISIS-related transactions occurred on the Binance exchange. Discovery into Binance’s internal records will thus likely uncover many other similar transactions and/or ways in which Defendants knowingly and substantially assisted ISIS.

---

<sup>21</sup> Plaintiffs’ approach to blockchain analysis is explained *supra* ¶¶ 389-391.

462. Reports corroborate ISIS’s use of cryptocurrency to raise funds and commit terrorist attacks. In addition to the many warnings discussed above that discuss ISIS, *supra* Part IV, additional examples follow.

463. As Ahmad Helmi Hasbi, a Research Analyst, and Remy Mahzam, an Associate Research Fellow at the International Centre for Political Violence & Terrorism Research from the S. Rajaratnam School of International Studies, reported in a 2018 article, a joint study by Indonesia’s National Counterterrorism Agency, State Intelligence Agency, and Financial Transaction Reports and Analysis Center “disclosed that online donations are the preferred method to finance terror groups because of its practicality. . . . In December 2017, US citizen Zoobia Shahnaz was charged [with] bank fraud and multiple counts of money laundering in an alleged attempt to transfer over US\$62,000 worth of Bitcoins and other cryptocurrencies abroad to fund the Islamic State terror group. Anti-terrorism hacktivist Ghost Security Group . . . . [u]ncovered several Bitcoin funding sites exploited by IS supporters on the dark web with a digital wallet containing \$3 million in Bitcoin value believed to have been used to finance the terror operation.”

464. In 2019, Megan McBride and Zack Gold, national security analysts at CNA, found that, like other terrorist groups that have “used cryptocurrencies to transfer funds and obtain goods,” “ISIS fighters in Syria have allegedly used cryptocurrencies to facilitate both international transactions and domestic purchases.” Indeed, “[r]eports indicate that ISIS purchased the weapons used in the 2015 Munich attacks on the dark web, and the owner of a website containing ISIS propaganda allegedly paid the site’s service provider in cryptocurrency.”

465. In 2020, the DOJ “announced the government’s largest-ever seizure of cryptocurrency in the terrorism context, stemming from the dismantling of terrorist financing

campaigns involving . . . ISIS,” which “had used cryptocurrency technology and social media platforms to spread [its] influence and raise funds for terror campaigns.”

466. Moreover, Blockchain analysis firm TRM Labs explained in 2022 that it had “recently uncovered evidence of direct cryptocurrency use for fundraising by an official ISIS affiliate”—the Islamic State in Khurasan (ISKP or ISIS-K), which is ISIS’s affiliate in Afghanistan. ISIS-K was “accepting cryptocurrency donations amid ramped up propaganda and recruitment efforts,” and TRM Labs “identified a Bitcoin, Ethereum and TRX (Tron) address controlled by ISKP’s media unit, the al-Azaim Foundation for Media.” TRM Labs thus concluded, “ISIS and its supporters in Central Asia are increasingly turning to virtual assets to move and raise funds.” Indeed, there are reports that ISIS-K “has been sent \$25,000 worth in cryptocurrency on a monthly basis” by ISIS affiliates in West Africa.

467. Throughout the Relevant Period, the United Nations has also repeatedly recognized ISIS’s embrace of cryptocurrency to finance its activities. *See supra* Part IV(D)(2).

468. In 2024, TRM Labs reported that its “research found a growing interest in and use of crypto by terrorist groups and their supporters to solicit donations and conduct cross-border payments. This includes ISIS and its affiliates in multiple countries around the world.”

469. As Treasury recognized in 2024, “an increasing number of ISIS affiliates experiment with using virtual assets to raise and transfer funds across multiple jurisdictions.” Treasury observed “the ISIS global network, including ISIS-West Africa, making payments using virtual assets, in particular the stablecoin Tether,” and Treasury has also “sanctioned two Egypt-based ISIS cybersecurity experts in part for providing guidance to ISIS leadership on the use of virtual assets.”

470. Moreover, Jessica Davis, a terrorism and illicit finance scholar, wrote in summer 2024 that “[g]lobally, terrorist groups have increasingly used cryptocurrency in recent years to move funds internationally, and the Islamic State is no exception.” As she explained, “Islamic State provinces and sub-groups are not the only ones using cryptocurrency; identity-based support networks also use it. . . . Islamic State supporters have also been sanctioned for providing Islamic State leadership and supporters with cybersecurity training and enabling the group’s use of cryptocurrency and obfuscation methods meant to hide the source and destination of the funds.” In particular, ISKP “has used Tether to receive funds, and recent attacks and arrests suggest a broad use of cryptocurrency by the group and its supporters. . . . While Afghanistan is not high on the index of crypto adoption, *hawaladars* in the country have been relatively quick to adopt cryptocurrency as a service, and proximity to India and Pakistan, both very high crypto-adopting countries, likely further facilitates this adoption. *Hawaladars* set up wallets to receive transfers of funds through cryptocurrency and essentially act as informal cryptocurrency exchanges and cash-out services.”

471. It is highly probable that a substantial percentage of ISIS’s cryptocurrency transactions during the Relevant Period moved through the Binance exchange because, among other reasons, it was the largest exchange by transaction volume that willfully (and completely) disregarded enforcing AML/CFT and KYC requirements during that time.

## **VII. Defendants’ Unlawful Conduct Had A Substantial Nexus To New York And The United States**

472. Defendants’ contacts with New York and the United States reflected a series of calculated choices made by Defendants, for which the throughline was simple: Defendants sought to—and did (until they got caught)—make tens of billions of dollars consciously pursuing a strategy in which the foundation of Binance’s terrorist finance-driven profit model was simple:

leverage the unrivaled, and value-additive, power of New York's banks, financial system, enterprises, markets, and customer-bases (crypto and non-crypto alike), while consciously defying New York (and United States) laws designed to prevent persons from abusing the U.S. financial system to fund terrorist attacks, including New York's (and the U.S.'s) rules and regulations governing Defendants' affirmative legal obligations arising under their Anti-Money Laundering/Counter-Financing of Terrorism duties (widely known by the acronyms "AML/CFT" and/or AML/CTF").

**A. Binance's Unlawful Conduct Had a Substantial Nexus to New York and the United States Through Binance's New York Contacts Under Rule 4(k)(1)(A)**

473. Defendants' scheme to finance the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and ISIS relied on substantial and deliberate contacts with New York that were critical to effectuating Defendants' scheme, which included their purposeful use of: (1) New York customers; (2) New York business partners; and (3) New York banks.

**1. Binance Used New York Customers in Carrying Out the Scheme**

474. As described further below and as set forth in prosecution and settlement documents between the DOJ, the CFTC, and the SEC against Binance and Zhao, several of Binance's key "VIP market makers" and largest customers were quantitative hedge funds that were headquartered in and directed trading from New York. These market makers provided critical and deliberately sought-after liquidity to Binance's international exchange, Binance.com, effectively fueling an unregulated marketplace that gave known terrorist groups, including al-Qaeda, ISIS, Hamas, PIJ, and the IRGC, the ability to freely trade and transfer cryptocurrency and accept direct donations. Binance deliberately reached out to these New York-based firms to cultivate their business and was aware of their location in New York.

475. From 2017-2024, Binance conducted massive amounts of business with New York-based counterparties, including the crypto exchanges Gemini (total transaction value approximately \$25 billion) and Paxful (\$3.7 billion). In addition, financial flows between Binance and New York-based Coinbase totaled \$240 billion during the same period. Like its dealings with New York-based market makers, Binance’s transactions with major New York-based crypto exchanges provided essential liquidity to its platform, helping make it the world’s largest cryptocurrency exchange and the preferred exchange of terrorist groups seeking liquidity.

## 2. **Binance Used New York Partners in Carrying Out the Scheme**

476. Binance also purposefully availed itself of the New York commercial system, relying on at least three New York-based partners to imbue Binance’s crimes with the legitimacy of the New York commercial system in the course of providing substantial assistance to the terrorist groups that attacked and injured Plaintiffs or their family members.

477. **Chainalysis.** In or about October of 2018, Binance reached into New York to partner with Chainalysis, a New York-based “cryptocurrency compliance and investigation” company, to “complete[] a global roll-out of its compliance solution [for] Binance ... to help address the challenges at the intersection of cryptocurrencies, regulators and traditional financial institutions.” In connection with the implementation of the Chainalysis “compliance solution,” then-CFO of Binance Wei Zhou told industry publication CoinDesk that he hoped the partnership with Chainalysis would inspire the crypto industry “to take anti-money laundering and anti-terrorism financing measures seriously.” Binance’s compliance program with Chainalysis was a sham: Binance used its purported compliance relationship with the New York-based Chainalysis to conceal its ongoing effort to facilitate both money laundering and terrorist finance.

478. **Refinitiv.** In late 2018, Binance also reached into New York to partner with New York-based Refinitiv to implement Refinitiv’s automated Know-Your-Customer (KYC) software “to integrate the World-Check Risk Intelligence database into [Binance’s] internal workflow” and “purportedly allow Binance to streamline the screening process for onboarding, KYC, and third-party risk due diligence.” As Binance admitted in its guilty plea, despite public representations to the contrary, the company did not use Refinitiv’s software to conduct genuine KYC or due diligence procedures: it intentionally “did not collect full KYC information from a large share of its users until May 2022” and allowed most users to open accounts without conducting any KYC or AML procedures at all. As it did with Chainalysis, Binance used its purported partnership with Refinitiv to create a false impression of regulatory compliance and conceal its unlawful assistance to terrorist groups.

479. **Paxos Trust Company.** In or about 2019, Binance reached into New York to solicit an ongoing business relationship with Paxos Trust Company (“Paxos”), a New York-based and -regulated limited purpose trust company. Together, Binance and Paxos issued a U.S. dollar-backed stablecoin, BUSD, the U.S. dollar reserves for which were maintained by Paxos in New York. Each BUSD stablecoin is equivalent to one U.S. dollar. Stablecoins pegged to the U.S. dollar can be used to move a derivative of U.S. dollars across borders without going through regulated U.S. banks that would otherwise monitor this activity. Similarly, stablecoins pegged to the U.S. dollar can be withdrawn into U.S. dollars. Binance and Paxos also had a profit-sharing agreement to invest those reserves for their mutual benefit.

480. The purpose of Binance’s solicitation of Paxos was to obtain a veneer of legitimacy from the highly respected New York Department of Financial Services (NYDFS), which regulated Paxos. In 2019, BUSD was authorized by NYDFS for trading on the Ethereum

blockchain. Binance made a point of touting this authorization by New York’s financial regulator in announcing and marketing BUSD, noting, for example, that NYDFS regulation “gives BUSD a higher level of trust and security than other stablecoins. As Binance’s former Chief Financial Officer explained, “[l]aunching a stablecoin approved by the New York State Department of Financial Services (NYDFS) is a strategic step for Binance to provide on-chain financial services for users across the world.” According to contemporary industry press coverage, “Binance chose to work with Paxos on the new stablecoin because they feel a stablecoin approved and regulated by the New York State Department of Financial Services, ensuring the utmost of consumer protections,” would help Binance expand its business vis a vis the then-dominant stablecoin, Tether. As one commentator put it, “[o]ne thing Binance USD will have that Tether doesn’t is the blessing of the State of New York.”

481. Binance’s effort to obtain and leverage the imprimatur of New York regulators worked: from an initial offering of less than 20 million BUSD in September 2019, by April 2020 the amount of BUSD in circulation exceeded 200 million. As of November 2022, Binance held nearly \$24 billion in New York-issued Paxos BUSD—about one-third of the company’s total crypto assets.

482. In 2023, the NYDFS “ordered Paxos to cease minting Paxos-issued BUSD as a result of several unresolved issues related to Paxos’ oversight of its relationship with Binance in regard to Paxos-issued BUSD.” According to the NYDFS, the agency took the action because Paxos “violated its obligation to conduct tailored, periodic risk assessments and due diligence refreshes of Binance and Paxos-issued BUSD customers to prevent bad actors from using the platform.”

483. Financial flows between Binance and Paxos from 2019 to 2024 were approximately \$40 billion.

484. Analysis of public blockchains showed that wallets owned by, or affiliated with, FTOs, including Hamas, involved transactions in BUSD.

### **3. Binance Used New York Banks in Carrying Out the Scheme**

485. Binance also purposefully availed itself of the New York banking system, relying on New York-based banks, including Signature Bank, to clear and settle payments of billions of U.S. dollars in the course of providing substantial assistance to the terrorist groups that attacked and injured Plaintiffs or their family members. Binance held numerous accounts at Signature Bank and extensively utilized the bank's Signet Platform to settle cryptocurrency transactions in U.S. dollars. Between 2019 and 2023, Binance deposited more than \$5.5 billion in its Signature Bank accounts.

486. New York prosecutors also pursued enforcement actions alerting Defendants that terrorist groups sought to leverage multinational corporations' choice to use the New York banking system. In 2009, for example, after New York regulators announced counterterrorism-related enforcement actions against European banks, the Manhattan District Attorney told Bloomberg that New York was prosecuting "big cases," including "[o]ne involving Lloyd's [of London], where they were taking Iranian money, stripping the identification, and then sending it to U.S. . . . correspondent banks to get dollars to buy equipment for weapons" and observed that "[p]eople"—even terrorists—"still want to be paid in dollars," which was "the reason they go through U.S. banks." In 2014, likewise, the Manhattan District Attorney warned multinational corporations that, "if you are going to use the American banking system, particularly New York, for your dollar clearing transactions, you are going to have to abide by [America's] rules."

**B. Alternatively, Binance’s Unlawful Conduct Had A Substantial Nexus To the United States Through Binance’s U.S.-Wide Contacts Under Rule 4(k)(2)<sup>22</sup>**

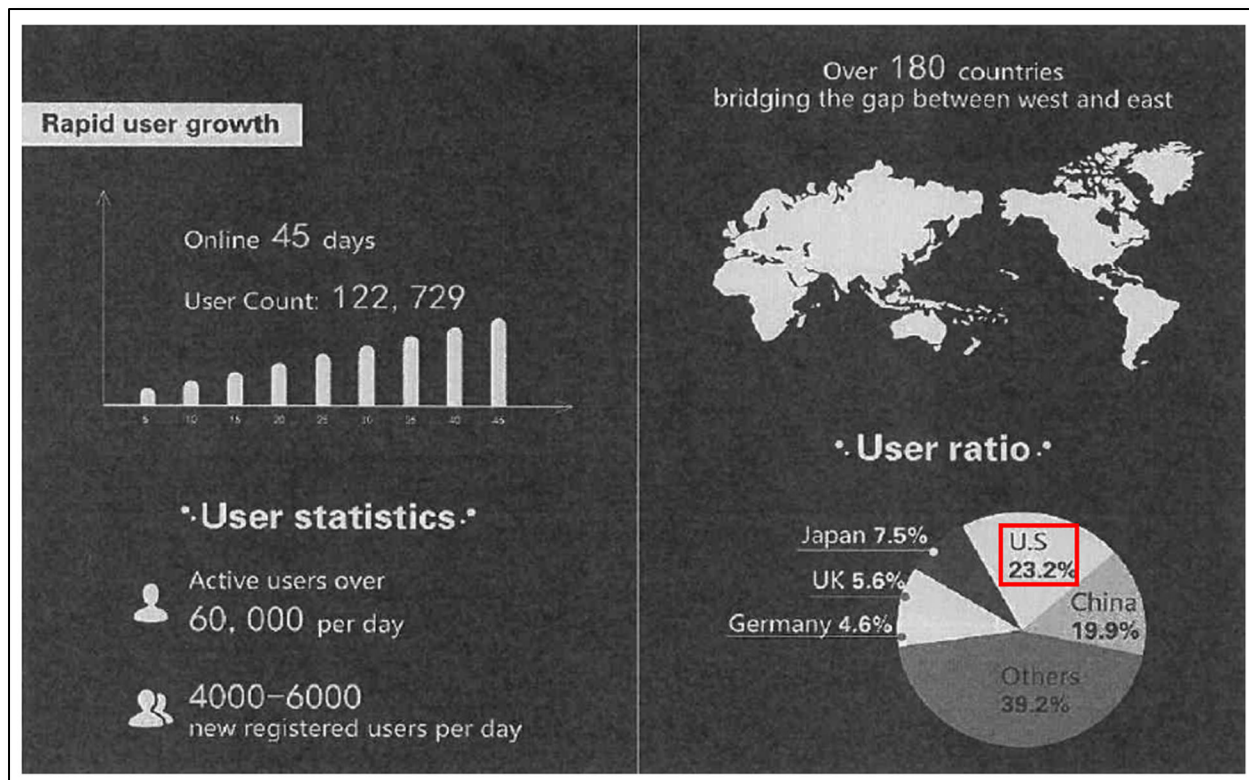
487. Alternatively, personal jurisdiction exists over Binance under Rule 4(k)(2) because Binance’s unlawful conduct had a substantial nexus to the United States as a forum through Binance’s U.S.-wide contacts based on Binance’s: (1) illegal operation of an unlicensed money transmitting business wholly or in substantial part in United States by serving a substantial number of U.S. users in the United States through Binance’s cryptocurrency exchange in the United States; (2) use of New York banks, New York customers, and New York business partners in carrying out Defendants’ scheme; and (3) use of one or more U.S.-based technology service provider(s) in carrying out Defendants’ scheme.

**1. Binance Illegally Operated an Unlicensed Money Transmitting Business Wholly or in Substantial Part in the United States by Serving a Substantial Number of U.S. Users**

488. In short, Binance has admitted that starting at least as early as August 2017 and continuing until at least October 19, 2022, Binance operated a cryptocurrency exchange wholly or in substantial part in the United States by serving a substantial number of U.S. users. For example, Binance has admitted: “From the beginning, [Binance] tracked and monitored the status and growth of its U.S.-registered users and its U.S.-based website visitors. In or around August 2017, [Binance] created a graphic [reproduced below, with red box added] touting the exchange’s ‘[r]apid user growth’ in its first forty-five days ..., showing that more than 23% of Binance’s 122,729 users were from the United States, a greater share than from any other country.”

---

<sup>22</sup> Rule 4(k)(2) is pled in the alternative in the event the Court determines that Binance is not otherwise subject to personal jurisdiction in New York or another State. The national contacts pled support jurisdiction under Rule 4(k)(2).



489. According to periodic revenue reports prepared by Binance personnel, as of January 2020 approximately 19.9% of Binance’s customers were located in the United States. By September 2020, Binance had approximately 2.5 million users in the U.S.—more than it had in any other country. According to Binance’s own transaction data, U.S. users conducted trillions of dollars in transactions on the platform between August 2017 and October 2022—transactions that generated over \$1.6 billion in profit for Binance.

490. According to Binance’s November 2023 settlement agreement with OFAC, “[f]rom approximately August 2017 to October 2022” Binance “matched and executed virtual currency trades on its online exchange platform between U.S. person users and users in sanctioned jurisdictions or blocked persons.” Upon information and belief, these U.S. person users included customers located in New York. Pursuant to Binance’s settlement with OFAC, these transactions, which constituted “direct or indirect exportation or other supply of goods and

services from the United States, or by U.S. persons, to users whom [Binance] identified through its Know Your Customer (KYC) process . . . as being [sanctioned entities or in sanctioned jurisdictions] . . . resulted in at least 1,667,153 virtual currency transactions – totaling approximately \$706,068,127.”

491. Binance has admitted to conspiring to operate as a virtual currency exchange to gain market share and profit by attracting “a substantial number of U.S. users” and “particularly U.S. VIP users, who accounted for a significant percentage of the overall trading volume on Binance.com.” Binance chose not to comply with U.S. legal and regulatory requirements because it determined that doing so would limit its ability to attract and maintain U.S. users, who were critical to the company’s viability and success. Binance deliberately concealed its avoidance of and noncompliance with U.S. law from U.S. regulators and law enforcement.

492. As a result of Binance’s decision not to implement comprehensive controls blocking illegal transactions between sanctioned users and U.S. users, Binance willfully caused transactions between U.S. users and users in comprehensively sanctioned jurisdictions in violation of U.S. law, including Iran and Syria. Specifically, between in or about January 2017 through May 2022, Binance caused at least 1.1 million transactions in violation of the International Emergency Economic Powers Act between users it had reason to believe were U.S. persons and persons it had reason to believe resided in Iran, with an aggregate transaction value of at least \$898,618,825.

493. In 2019, then-CEO Zhao admitted that “there are a bunch of laws in the US that prevent Americans from having any kind of transaction with any terrorist,” compliance with which would require Binance to “submit all relevant documents for review” by U.S. regulators. Zhao and Binance intentionally declined to institute effective compliance with those U.S. laws,

refusing “to implement procedures to determine whether a customer appears on lists of known or suspected terrorists or terrorist organizations” and thereby willfully enabling U.S. users to transact with known or suspected terrorists. To the extent Binance instituted compliance procedures, it intentionally did so inadequately, such that “users in the United States and from comprehensively sanctioned countries continued to access Binance.com, and Binance’s matching engine continued to cause transactions between U.S. persons and users in comprehensively sanctioned jurisdictions, in violation of U.S. law.”

494. In this connection, Binance has admitted that known terrorist groups, including Hamas, use Binance to raise and transfer funds, and Binance user addresses have been found to interact with bitcoin wallets associated with al-Qaeda, ISIS, Hamas, PIJ, and the IRGC. On information and belief, those terrorist wallets interacted with Binance users in the United States.

## **2. Binance Used U.S. Banks, U.S. Customers, and U.S. Business Partners in Carrying Out Defendants’ Scheme**

495. As discussed, *see* Part VII(A), Binance also used U.S. banks, had U.S. customers, and used U.S. partners, including banks, customers, and partners located in New York, to carry out its illicit scheme.

## **3. Binance Used One or More U.S.-Based Technology Service Provider(s) in Carrying Out Defendants’ Scheme**

496. In addition to many other purposeful connections to the United States, Binance contracts with U.S.-based Amazon Web Services to host the Binance.com website through which the illegal transactions occurred and obtain other web-related services; leases office space in the United States for its employees; procures legal and business advice from U.S. law firms and consultants; and both hosts and attends networking and social events in the United States, including an April 2022 party in Las Vegas to which Binance invited its ‘largest accounts’ ... and a networking event in Austin, Texas.” All these contacts were part of Binance’s effort to

exploit and leverage the U.S. market, without which Binance could not have achieved the scale and liquidity necessary to make it the world's largest crypto exchange and the preferred exchange for terrorists.

**C. Zhao's Unlawful Conduct Had a Substantial Nexus to New York and the United States**

497. Defendant Zhao conceived and founded Binance, made strategic decisions for it and has admitted that he “exercised day-to-day control over its operations and finances.” He has “ultimately controlled all of Binance’s business activities at all times” since 2017, and has “directly or indirectly owned the scores of entities that operate the Binance platform.” In this capacity, Zhao has been responsible for all major strategic decisions, business development, and management of the minutiae of Binance’s operations, including directing and overseeing the creation and operation of Binance’s critical operations (such as the operations of Binance’s trade matching engines, websites, API functionalities, and order entry system) and has been involved in and ultimately retained control over all critical decisions for the enterprise, including Binance’s failure to implement and enforce anti-money laundering controls and Know Your Customer procedures.

498. Zhao specifically played a substantial role in directing Binance’s efforts to exploit the U.S. market, retain key U.S. “VIP” users, and circumvent the U.S. regulatory regime, including by “encouraging [U.S.] users to obfuscate their U.S. connections . . . by creating new accounts and [falsely] submitting non-U.S. KYC information in connection with those accounts.”

499. By virtue of Zhao’s dominant role in Binance, including its strategies to exploit and leverage the New York and United States markets while circumventing governing financial regulations, Binance’s purposeful availment of New York and the United States as detailed above is equally attributable to Zhao.

**VIII. Plaintiffs Were Killed Or Injured In Terrorist Attacks Committed, Planned, Or Authorized By Foreign Terrorist Organizations That Defendants Supported**

**A. The IRGC-Sponsored Attacks by Hezbollah and Kataib Hezbollah in Iraq**

**1. The November 7, 2022 Hostage-Taking Attack in Iraq (Troell Family)**

500. On November 7, 2022, a joint cell comprised of Lebanese Hezbollah and JAM, which was funded, armed, and logistically supported by the IRGC, committed hostage-taking attack involving small arms in Baghdad, Iraq (the “November 7, 2022 Attack”).

501. The November 7, 2022 Attack was planned and authorized by Hezbollah.

502. The November 7, 2022 Attack was aided by IRGC-funded and supplied bounty payments and martyr payments to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; both types of payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the November 7, 2022 Attack.

503. The November 7, 2022 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

504. The November 7, 2022 Attack furthered the Axis Conspiracy by demonstrating the IRGC’s (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC’s, Binance’s, and Zhao’s ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC’s ability to collect the highest prices for Axis Payments depended upon the IRGC’s reputation for violence, which was bolstered by November 7, 2022 Attack given its high-profile nature.

505. **Stephen Troell** was in Iraq driving home at the time of the attack, when the terrorists attempted to seize Stephen for ransom. Stephen Troell was injured in the November 7, 2022 Attack. Stephen Troell died on November 7, 2022, as a result of injuries sustained during the attack.

506. Stephen Troell was a U.S. national at the time of the attack and his death.

507. Plaintiff Jocelyn Troell is the widow of Stephen Troell and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Stephen Troell's estate.

508. As a result of the November 7, 2022 Attack and Stephen Troell's injuries and death, each member of the Troell Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Stephen Troell's society, companionship, and counsel.

509. As a result of the November 7, 2022 Attack, Stephen Troell was injured in his person and/or property. The Plaintiff members of the Troell Family are the survivors and/or heirs of Stephen Troell and are entitled to recover for the damages Stephen Troell sustained.

## **2. The December 27, 2019 Rocket Attack in Iraq (Hamid Family)**

510. On December 27, 2019, a joint cell comprised of Hezbollah and Kataib Hezbollah, for which the IRGC, including IRGC-QF and IRGC-IO, provided funding, training, weapons, logistical support, and intelligence, committed a rocket attack in Kirkuk, Iraq (the "December 27, 2019 Attack").

511. The December 27, 2019 Attack was personally planned and authorized by, *inter alia*, Hezbollah, the IRGC-QF, including Qasem Soleimani, and Kataib Hezbollah, including dual-hatted IRGC/Kataib Hezbollah terrorist Abu Mahdi al-Muhandis.

512. The December 27, 2019 Attack was aided by IRGC-funded and supplied bounty payments and martyr payments to operatives from the IRGC, Hezbollah, and Kataib Hezbollah;

both types of payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the December 27, 2019 Attack.

513. The December 27, 2019 Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made rockets, rocket launchers, artillery computer systems, optics, drones, and satellite imagery, which the IRGC (through the IRGC-QF and the IRGC-IO) made available to Hezbollah and Kataib Hezbollah.

514. The December 27, 2019 Attack relied upon IRGC-supplied intelligence, including, but not limited to, intelligence from IRGC-supplied drones and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah, as well as Hezbollah's and Kataib Hezbollah's terrorists on the ground in Kirkuk, who served as the IRGC's, Hezbollah's, and Kataib Hezbollah's intelligence eyes and ears in the area.

515. The December 27, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

516. The December 27, 2019 Attack furthered the Axis Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by December 27, 2019 Attack given its high-profile nature.

517. **Nawres Hamid** was in Iraq as a civilian government contractor working for Valiant Integrated Services LLC at the time of the attack. Nawres Hamid was injured in the December 27, 2019 Attack. Nawres Hamid died on December 27, 2019, as a result of injuries sustained during the attack.

518. Nawres Hamid was a U.S. national at the time of the attack and his death.

519. Plaintiff Noor Alkhalili is the widow of Nawres Hamid and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Nawres Hamid's estate.

520. Plaintiff A.W., by and through his next friend Noor Alkhalili, is the minor son of Nawres Hamid. He is a U.S. national.

521. Plaintiff H.W., by and through his next friend Noor Alkhalili, is the minor son of Nawres Hamid. He is a U.S. national.

522. As a result of the December 27, 2019 Attack and Nawres Hamid's injuries and death, each member of the Hamid Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Nawres Hamid's society, companionship, and counsel.

523. As a result of the December 27, 2019 Attack, Nawres Hamid was injured in his person and/or property. The Plaintiff members of the Hamid Family are the survivors and/or heirs of Nawres Hamid and are entitled to recover for the damages Nawres Hamid sustained.

### **3. The January 8, 2020 Attack in Iraq (Al Asad Air Base Attack)**

524. On January 8, 2020, a combined terrorist group comprised of IRGC terrorists in Iran drawn from the IRGC-QF, IRGC-IO, and IRGC-Missile Command, and a joint Hezbollah/Kataib Hezbollah cell in Iraq, committed a complex attack targeting the United States and Americans at Al Asad Air Base in Anbar, Iraq, which attack began at around 1:30 A.M. local Iraq time and lasted more than three hours, and featured waves of IRGC missile attacks that

were supported by Hezbollah and Kataib Hezbollah drones in Iraq and IRGC satellites in orbit, complemented by a local Kataib Hezbollah ground assault team consisting of more than twenty Kataib Hezbollah terrorists who, on information and belief, deployed a comprehensive mix of IRGC-supplied weapons, including, but not limited to, IRGC-supplied drones, RPGs, RPG optics, mortars, artillery optics, small arms, night-vision optics, and communications systems, among other weapons (the “January 8, 2020 Attack”).

525. The January 8, 2020 Attack was personally planned and authorized by, *inter alia*, Hezbollah, the IRGC-QF, including Qasem Soleimani and Mohsen Rezai, and Kataib Hezbollah, including dual-hatted IRGC/Kataib Hezbollah terrorist Abu Mahdi al-Muhandis.

526. The January 8, 2020 Attack was aided by IRGC-funded and supplied bounty payments and martyr payments to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; both types of payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the January 8, 2020 Attack. For example, on information and belief, a U.S. airstrike during the January 8, 2020 Attack killed all or nearly all of the on-the-ground Kataib Hezbollah terrorists; thereafter, under standard IRGC tradecraft and practice, the Qods Force likely used IRGC funds to make martyr payments to the family members related to each such Kataib Hezbollah terrorist whom U.S. forces “martyred” in self-defense during the January 8, 2020 Attack.

527. The January 8, 2020 Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made missiles, drones, satellites, RPGs, RPG optics, mortars, artillery optics, small arms, night-vision optics, and communications systems, among other weapons, which the IRGC used and made available (through the IRGC-QF and the IRGC-IO) to Hezbollah and Kataib Hezbollah.

528. The January 8, 2020 Attack relied upon IRGC-supplied and Kataib Hezbollah-supplied intelligence, including, but not limited to: (1) IRGC-supplied imagery of Al-Asad Air Base through IRGC-made drones and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah to maximize the lethality of the attack; (2) Kataib Hezbollah-supplied human intelligence through Kataib Hezbollah's embedded terrorists who worked inside Al-Asad Air Base undercover for certain Iraqi contractors there and served as the IRGC's, Hezbollah's, and Kataib Hezbollah's intelligence eyes and ears at the Air Base; and (3) on information and belief, Hezbollah's and Kataib Hezbollah's network of child terrorists in Iraq, whom Hezbollah and Kataib Hezbollah deployed to ring U.S. bases in Iraq, including Al-Asad Air Base, to develop pattern of life intelligence, which maximized the lethality of the January 8, 2020 Attack.

529. The January 8, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, many victims of this attack were civilians not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

530. From January 2019 through January 2021, the U.S. government, Iranian regime, IRGC, and mainstream media outlets publicly reported, *inter alia*:

- a. On February 8, 2019, IRGC media arm *Fars News Agency* reported that Ayatollah Khamenei published a tweet on Twitter that tagged President Trump's personal Twitter account, and publicly disclaimed the notion of any conflict between the nation of Iran and the nation of the United States by asserting that the Ayatollah and the IRGC targeted the U.S. government, not the United States as a nation: "a post on the Arabic [Twitter] account of ... Ali Khamenei ... said that chants against the US are aimed at Washington's officials like Donald Trump, John Bolton, and Mike Pompeo. The tweet was addressed to US President Donald Trump and two other American top officials, reading 'Down with USA means down with Donald Trump, John Bolton and Mike Pompeo,' and not the American nation."
- b. On October 25, 2019, Treasury publicly emphasized that the nation of the United States was never in conflict with the nation of Iran, stating: "U.S. government efforts are

directed at the Iranian regime. They are not directed at the people of Iran, who themselves are victims of the regime's ... corruption." In so doing, Treasury was repeating a long-held view of the U.S. government. On October 25, 2007, for example, U.S. officials expressly rejected the assertion that America was in an "armed conflict with Iran" during an interview with the *New York Times* shortly after the United States designated the Qods Force as an SDGT based upon its sponsorship of terrorist attacks targeting U.S. servicemembers in Iraq and Afghanistan.

- c. On January 2, 2020, President Trump stated, in reference Qasem Soleimani's death: "We took action last night to stop a war. We did not take action to start a war." In the days that followed, he reiterated that point. On January 4, 2020, the *Associated Press* reported: "Iran has vowed harsh retaliation, raising fears of an all-out war. U.S. President Donald Trump says he ordered the strike to prevent a conflict." On January 5, 2020, the *Associated Press* reported: "Mr Trump says he ordered the strike, a high-risk decision that was made without consulting Congress or US allies, to prevent a conflict."
- d. On January 8, 2020, alongside its January 8, 2020 Attack, the IRGC launched a coordinated disinformation campaign that the IRGC intentionally designed, consistent with IRGC tradecraft, to target American military families in the United States whose loved ones were involved in the attack at Al-Asad by falsely claiming, as IRGC-controlled IRIB did, that: "More than 80 U.S. forces have reportedly been killed during Iranian missile strikes to intended U.S. targets in Iraq on [January 8, 2020], IRIB quoted a source close to ... [the] IRGC." In so doing, the IRGC deliberately sought to leverage what it correctly understood would likely be a 12-24 hour period when (a) the IRGC knew it had not killed any American servicemembers in Iraq but (b) given the time zone differences and post-attack chaos, the families back home could be terrorized for at least a while. The IRGC and Hezbollah regularly deployed similar terroristic tactics against the Israeli military and Israeli military families, famously doing so repeatedly during Hezbollah's fighting with Israel in 2006.
- e. On June 29, 2020, *Reuters* reported that the U.S. government and IRGC were brought "to the brink of armed conflict after Iran retaliated by firing missiles at American targets."
- f. On June 29, 2020, *Reuters* reported that: "Iran has issued an arrest warrant for U.S. President Donald Trump and 35 others over the killing of top general Qassem Soleimani and has asked Interpol for help, Tehran prosecutor Ali Alqasimehr said... Alqasimehr said the warrants had been issued on charges of murder and terrorist action. He said Iran had asked Interpol to issue a 'red notice' seeking the arrest of Trump and the other individuals [Iran] accuses of taking part in the killing of Soleimani."
- g. On December 5, 2020, IRGC media arm *Mehr News Agency* reported: "The act of terror was carried out under the direction of US President Donald Trump, with the Pentagon taking responsibility for the strike."
- h. On January 14, 2020, President Trump implemented Executive Order 13,902, which imposed additional counterterrorism sanctions on the IRGC that targeted its use of missiles to commit terrorist attacks: "[The President] find[s] that Iran continues to be the

world's leading sponsor of terrorism and that Iran has threatened United States military assets and civilians through the use of military force and support to Iranian-backed militia groups. It remains the policy of the United States to deny Iran all paths to a nuclear weapon and intercontinental ballistic missiles, and to counter the totality of Iran's malign influence in the region. In furtherance of these objectives, it is the policy of the United States to deny the Iranian government revenues, including revenues derived from the export of products from key sectors of Iran's economy, that may be used to fund and support its nuclear program, missile development, terrorism and terrorist proxy networks, and malign regional influence."

- i. In December 2021, the State Department reported to Congress in *Country Reports on Terrorism 2020* that: "Significant terrorist incidents [in 2020] included" when "Houthi militants attacked Riyadh using ballistic missiles and multiple UAS [i.e., drones]" on "September 10, [2020]."

531. The January 8, 2020 Attack furthered the Axis Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by January 8, 2020 Attack given its high-profile nature.

532. **Staff Sergeant Toni Alexander** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SSG Alexander, who suffered from traumatic brain injury ("TBI"), PTSD, anxiety, depression, panic disorder, insomnia, sleep apnea, tinnitus, and migraines.

533. As a result of the January 8, 2020 Attack and her injuries, SSG Alexander has experienced severe physical and emotional pain and suffering.

534. Plaintiff SSG Alexander was a U.S. national at the time of the attack and remains one today.

535. Plaintiff Brock Johnson is the husband of SSG Alexander and a U.S. national.

536. As a result of the January 8, 2020 Attack and SSG Alexander's injuries, the Plaintiff members of the Alexander Family have experienced severe mental anguish as well as emotional pain and suffering.

537. **Sergeant Shanerria Barber** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Barber, who suffered from TBI, PTSD, anxiety, depression, insomnia, tinnitus, and multiple sclerosis.

538. Plaintiff SGT Barber was a U.S. national at the time of the attack and remains one today.

539. As a result of the January 8, 2020 Attack and her injuries, SGT Barber has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

540. **Specialist Patrick Ben** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Ben, who suffered from TBI, hyperthyroidism, Graves' disease, and thyroid toxicosis paralysis.

541. Plaintiff SPC Ben was a U.S. national at the time of the attack and remains one today.

542. As a result of the January 8, 2020 Attack and his injuries, SPC Ben has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

543. **Specialist Badekemi Biladjetan** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Biladjetan, who suffered from TBI, PTSD, anxiety, depression, panic disorder, insomnia, eye convergence insufficiency, and migraines.

544. Plaintiff SPC Biladjetan was a U.S. national at the time of the attack and remains one today.

545. As a result of the January 8, 2020 Attack and her injuries, SPC Biladjetan has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

546. **Specialist Einreb Bismanos** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Bismanos, who suffered from TBI.

547. Plaintiff SPC Bismanos was a U.S. national at the time of the attack and remains one today.

548. As a result of the January 8, 2020 Attack and his injuries, SPC Bismanos has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

549. **Sergeant Julius Brisco** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Brisco, who suffered from TBI, PTSD, depression, sleep apnea, tinnitus, and migraines.

550. As a result of the January 8, 2020 Attack and his injuries, SGT Brisco has experienced severe physical and emotional pain and suffering.

551. Plaintiff SGT Brisco was a U.S. national at the time of the attack and remains one today.

552. Plaintiff Melissa Brisco is the wife of Julius Brisco and a U.S. national.

553. Plaintiff T.B., by and through his next friend SGT Brisco, is the minor son of SGT Brisco and is a U.S. national.

554. Plaintiff J.M., by and through his next friend Melissa Brisco, is the minor stepson of SGT Brisco and is a U.S. national. J.M. lived in the same household as SGT Brisco for a substantial period and considered SGT Brisco the functional equivalent of a biological father.

555. As a result of the January 8, 2020 Attack and SGT Brisco's injuries, the Plaintiff members of the Brisco Family have experienced severe mental anguish as well as emotional pain and suffering.

556. **Specialist Ali Brown** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Brown, who suffered from TBI and anxiety.

557. Plaintiff SPC Brown was a U.S. national at the time of the attack and remains one today.

558. As a result of the January 8, 2020 Attack and her injuries, SPC Brown has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

559. **Sergeant Timothy Brown** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Brown, who suffered from TBI.

560. Plaintiff SGT Brown was a U.S. national at the time of the attack and remains one today.

561. As a result of the January 8, 2020 Attack and his injuries, SGT Brown has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

562. **Specialist James Carson** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Carson, who suffered from TBI, PTSD, anxiety, depression, and tinnitus.

563. As a result of the January 8, 2020 Attack and his injuries, SPC Carson has experienced severe physical and emotional pain and suffering.

564. Plaintiff SPC Carson was a U.S. national at the time of the attack and remains one today.

565. Plaintiff Mackenzie Harlow is the ex-wife of SPC Carson and a U.S. national.

566. As a result of the January 8, 2020 Attack and SPC Carson's injuries, the Plaintiff members of the Carson Family have experienced severe mental anguish as well as emotional pain and suffering.

567. **Specialist Mackenzie Harlow** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Harlow, who suffered from TBI, anxiety, tinnitus, migraines, and acute stress disorder.

568. As a result of the January 8, 2020 Attack and her injuries, SPC Harlow has experienced severe physical and emotional pain and suffering.

569. Plaintiff SPC Harlow was a U.S. national at the time of the attack and remains one today.

570. Plaintiff James Carson is the ex-husband of SPC Harlow and a U.S. national.

571. As a result of the January 8, 2020 Attack and SPC Harlow's injuries, the Plaintiff members of the Harlow Family have experienced severe mental anguish as well as emotional pain and suffering.

572. **Specialist Jaron Carter** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Carter, who suffered from TBI and PTSD.

573. As a result of the January 8, 2020 Attack and his injuries, SPC Carter has experienced severe physical and emotional pain and suffering.

574. Plaintiff SPC Carter was a U.S. national at the time of the attack and remains one today.

575. Plaintiff Olivia Carter is the wife of SPC Carter and a U.S. national.

576. Plaintiff J.C., by and through her next friend SPC Carter, is the minor daughter of SPC Carter. She is a U.S. national.

577. As a result of the January 8, 2020 Attack and SPC Carter's injuries, the Plaintiff members of the Carter Family have experienced severe mental anguish as well as emotional pain and suffering.

578. **Chief Warrant Officer 2 Thomas Caudill** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded CW2 Caudill, who suffered from TBI and tinnitus.

579. As a result of the January 8, 2020 Attack and his injuries, CW2 Caudill has experienced severe physical and emotional pain and suffering.

580. Plaintiff CW2 Caudill was a U.S. national at the time of the attack and remains one today.

581. Plaintiff Adrienne Caudill is the wife of CW2 Caudill and a U.S. national.

582. Plaintiff L.M.C., by and through his next friend CW2 Caudill, is the minor son of CW2 Caudill. He is a U.S. national.

583. Plaintiff L.S.C., by and through his next friend CW2 Caudill, is the minor son of CW2 Caudill. He is a U.S. national.

584. Plaintiff O.C., by and through his next friend CW2 Caudill, is the minor son of CW2 Caudill. He is a U.S. national.

585. Plaintiff R.C., by and through her next friend CW2 Caudill, is the minor daughter of CW2 Caudill. She is a U.S. national.

586. As a result of the January 8, 2020 Attack and CW2 Caudill's injuries, the Plaintiff members of the Caudill Family have experienced severe mental anguish as well as emotional pain and suffering.

587. **Chief Warrant Officer 2 Dolphise Colomb** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded CW2 Colomb, who suffered from TBI, PTSD, anxiety, insomnia, tinnitus, migraines, low testosterone, balance issues, cognitive communication disorder, speech issues, memory issues, and concentration issues.

588. As a result of the January 8, 2020 Attack and his injuries, CW2 Colomb has experienced severe physical and emotional pain and suffering.

589. Plaintiff CW2 Colomb was a U.S. national at the time of the attack and remains one today.

590. Plaintiff M.W., by and through his next friend CW2 Colomb, is the minor son of CW2 Colomb. He is a U.S. national.

591. As a result of the January 8, 2020 Attack and CW2 Colomb's injuries, the Plaintiff members of the Colomb Family have experienced severe mental anguish as well as emotional pain and suffering.

592. **Sergeant Quintin Copeland** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Copeland, who suffered from TBI, anxiety, and behavioral health issues.

593. As a result of the January 8, 2020 Attack and his injuries, SGT Copeland has experienced severe physical and emotional pain and suffering.

594. Plaintiff SGT Copeland was a U.S. national at the time of the attack and remains one today.

595. Plaintiff Tayana Roman is the ex-wife of Quintin Copeland and a U.S. national.

596. As a result of the January 8, 2020 Attack and SGT Copeland's injuries, the Plaintiff members of the Copeland Family have experienced severe mental anguish as well as emotional pain and suffering.

597. **Specialist Necollier Daniels** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Daniels, who suffered from TBI.

598. As a result of the January 8, 2020 Attack and his injuries, SPC Daniels has experienced severe physical and emotional pain and suffering.

599. Plaintiff SPC Daniels was a U.S. national at the time of the attack and remains one today.

600. Plaintiff Sarah Daniels is the wife of SPC Daniels and a U.S. national.

601. Plaintiff C.M.D., by and through his next friend SPC Daniels, is the minor son of SPC Daniels. He is a U.S. national.

602. Plaintiff C.T.D., by and through his next friend SPC Daniels, is the minor son of SPC Daniels. He is a U.S. national.

603. As a result of the January 8, 2020 Attack and SPC Daniels's injuries, the Plaintiff members of the Daniels Family have experienced severe mental anguish as well as emotional pain and suffering.

604. **Sergeant Jacob Deer** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Deer, who suffered from TBI.

605. As a result of the January 8, 2020 Attack and his injuries, SGT Deer has experienced severe physical and emotional pain and suffering.

606. Plaintiff SGT Deer was a U.S. national at the time of the attack and remains one today.

607. Plaintiff Samantha Deer is the wife of SGT Deer and a U.S. national.

608. Plaintiff J.A.S.D., by and through his next friend SGT Deer, is the minor son of SGT Deer. He is a U.S. national.

609. Plaintiff J.C.B.D., by and through his next friend SGT Deer, is the minor son of SGT Deer. He is a U.S. national.

610. As a result of the January 8, 2020 Attack and SGT Deer's injuries, the Plaintiff members of the Deer Family have experienced severe mental anguish as well as emotional pain and suffering.

611. **Specialist Corey Faucett** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Faucett, who suffered from TBI, PTSD, and anxiety.

612. Plaintiff SPC Faucett was a U.S. national at the time of the attack and remains one today.

613. As a result of the January 8, 2020 Attack and his injuries, SPC Faucett has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

614. **Thomas Feldschneider** was in Iraq as a civilian government contractor working for General Atomics at the time of the attack. The January 8, 2020 Attack severely wounded Thomas Feldschneider, who suffered from TBI, PTSD, anxiety, and insomnia.

615. As a result of the January 8, 2020 Attack and his injuries, Thomas Feldschneider has experienced severe physical and emotional pain and suffering.

616. Plaintiff Thomas Feldschneider was a U.S. national at the time of the attack and remains one today.

617. Plaintiff Courtney Feldschneider is the wife of Thomas Feldschneider and a U.S. national.

618. Plaintiff J.F., by and through his next friend Thomas Feldschneider, is the minor son of Thomas Feldschneider. He is a U.S. national.

619. Plaintiff N.S., by and through his next friend Kimberly Starnes, is the minor stepson of Thomas Feldschneider. He is a U.S. national. N.S. lived in the same household as Thomas Feldschneider for a substantial period and considered Thomas Feldschneider the functional equivalent of a biological father.

620. As a result of the January 8, 2020 Attack and Thomas Feldschneider's injuries, the Plaintiff members of the Feldschneider Family have experienced severe mental anguish as well as emotional pain and suffering.

621. **Sergeant Julie Ferguson** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT J. Ferguson, who suffered from TBI, PTSD, anxiety, depression, insomnia, tinnitus, and migraines.

622. Plaintiff SGT J. Ferguson was a U.S. national at the time of the attack and remains one today.

623. As a result of the January 8, 2020 Attack and her injuries, SGT J. Ferguson has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

624. **Sergeant Mitchell Ferguson** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Ferguson, who suffered from TBI, PTSD, anxiety, and tinnitus.

625. Plaintiff SGT Ferguson was a U.S. national at the time of the attack and remains one today.

626. As a result of the January 8, 2020 Attack and his injuries, SGT Ferguson has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

627. **Specialist Miguel Figueroa** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Figueroa, who suffered from TBI, PTSD, depression, and migraines.

628. Plaintiff SPC Figueroa was a U.S. national at the time of the attack and remains one today.

629. As a result of the January 8, 2020 Attack and his injuries, SPC Figueroa has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

630. **Sergeant Steven Garrett** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Garrett, who suffered from TBI, PTSD, anxiety, depression, tinnitus, and an erectile dysfunction due to prescribed antidepressant medication.

631. As a result of the January 8, 2020 Attack and his injuries, SGT Garrett has experienced severe physical and emotional pain and suffering.

632. Plaintiff SGT Garrett was a U.S. national at the time of the attack and remains one today.

633. Plaintiff Heather Garrett is the wife of SGT Garrett and a U.S. national.

634. Plaintiff S.G., by and through his next friend SGT Garrett, is the minor son of SGT Garrett. He is a U.S. national.

635. As a result of the January 8, 2020 Attack and SGT Garrett's injuries, the Plaintiff members of the Garrett Family have experienced severe mental anguish as well as emotional pain and suffering.

636. **Private Second Class Brandon Godwin** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded PV2 Godwin, who suffered from TBI and a shoulder injury.

637. Plaintiff PV2 Godwin was a U.S. national at the time of the attack and remains one today.

638. As a result of the January 8, 2020 Attack and his injuries, PV2 Godwin has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

639. **Sergeant Dustin Graham** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Graham, who suffered from TBI, PTSD, anxiety, depression, tinnitus, and migraines.

640. As a result of the January 8, 2020 Attack and his injuries, SGT Graham has experienced severe physical and emotional pain and suffering.

641. Plaintiff SGT Graham was a U.S. national at the time of the attack and remains one today.

642. Plaintiff Malissa Graham is the wife of SGT Graham and a U.S. national.

643. Plaintiff H.G., by and through her next friend SGT Graham, is the minor daughter of SGT Graham. She is a U.S. national.

644. Plaintiff J.G., by and through her next friend SGT Graham, is the minor daughter of SGT Graham. She is a U.S. national.

645. As a result of the January 8, 2020 Attack and SGT Graham's injuries, the Plaintiff members of the Graham Family have experienced severe mental anguish as well as emotional pain and suffering.

646. **Sergeant Stephon Green** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Green, who suffered from TBI, PTSD, anxiety, depression, tinnitus, and migraines.

647. As a result of the January 8, 2020 Attack and his injuries, SGT Green has experienced severe physical and emotional pain and suffering.

648. Plaintiff SGT Green was a U.S. national at the time of the attack and remains one today.

649. Plaintiff Mentoria Green is the wife of SGT Green and a U.S. national.

650. Plaintiff A.G., by and through his next friend SGT Green, is the minor son of SGT Green. He is a U.S. national.

651. Plaintiff S.G., by and through her next friend SGT Green, is the minor daughter of SGT Green. She is a U.S. national.

652. As a result of the January 8, 2020 Attack and SGT Green's injuries, the Plaintiff members of the Green Family have experienced severe mental anguish as well as emotional pain and suffering.

653. **Specialist Nathan Grosse** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Grosse, who suffered from TBI, PTSD, anxiety, depression, panic disorder, insomnia, tinnitus, migraines, and severe alcohol abuse disorder.

654. Plaintiff SPC Grosse was a U.S. national at the time of the attack and remains one today.

655. As a result of the January 8, 2020 Attack and his injuries, SPC Grosse has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

656. **Specialist Brett Gustafson** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Gustafson, who suffered from TBI, anxiety, and depression.

657. As a result of the January 8, 2020 Attack and his injuries, SPC Gustafson has experienced severe physical and emotional pain and suffering.

658. Plaintiff SPC Gustafson was a U.S. national at the time of the attack and remains one today.

659. Plaintiff Amanda Gustafson is the wife of SPC Gustafson and a U.S. national.

660. Plaintiff L.G., by and through his next friend SPC Gustafson, is the minor son of SPC Gustafson. He is a U.S. national.

661. As a result of the January 8, 2020 Attack and SPC Gustafson's injuries, the Plaintiff members of the Gustafson Family have experienced severe mental anguish as well as emotional pain and suffering.

662. **Captain Geoffrey Hansen** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded CPT Hansen, who suffered from TBI, PTSD, anxiety, depression, insomnia, tinnitus, and migraines.

663. As a result of the January 8, 2020 Attack and his injuries, CPT Hansen has experienced severe physical and emotional pain and suffering.

664. Plaintiff CPT Hansen was a U.S. national at the time of the attack and remains one today.

665. Plaintiff Allie Hansen is the wife of CPT Hansen and a U.S. national.

666. As a result of the January 8, 2020 Attack and CPT Hansen's injuries, the Plaintiff members of the Hansen Family have experienced severe mental anguish as well as emotional pain and suffering.

667. **Chief Warrant Officer 2 John Hergert** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded CW2 Hergert, who suffered from a TBI.

668. As a result of the January 8, 2020 Attack and his injuries, CW2 Hergert has experienced severe physical and emotional pain and suffering.

669. Plaintiff CW2 Hergert was a U.S. national at the time of the attack and remains one today.

670. Plaintiff Alyssa Hergert is the wife of CW2 Hergert and a U.S. national.

671. Plaintiff C.H., by and through his next friend CW2 Hergert, is the minor son of CW2 Hergert. He is a U.S. national.

672. As a result of the January 8, 2020 Attack and CW2 Hergert's injuries, the Plaintiff members of the Hergert Family have experienced severe mental anguish as well as emotional pain and suffering.

673. **Staff Sergeant Costin Herwig** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SSG Herwig, who suffered from TBI, PTSD, anxiety, depression, insomnia, bilateral vestibular system damage, tinnitus, and migraines.

674. As a result of the January 8, 2020 Attack and his injuries, SSG Herwig has experienced severe physical and emotional pain and suffering.

675. Plaintiff SSG Herwig was a U.S. national at the time of the attack and remains one today.

676. Plaintiff Jennifer Deaver is the wife of SSG Herwig and a U.S. national.

677. Plaintiff J.H., by and through his next friend SSG Herwig, is the minor son of SSG Herwig. He is a U.S. national.

678. Plaintiff J.F.D., by and through his next friend Jennifer Deaver, is the minor stepson of SSG Herwig and is a U.S. national. J.F.D. lived in the same household as SSG Herwig for a substantial period and considered SSG Herwig the functional equivalent of a biological father.

679. Plaintiff J.X.D., by and through his next friend Jennifer Deaver, is the minor stepson of SSG Herwig and is a U.S. national. J.X.D. lived in the same household as SSG Herwig for a substantial period and considered SSG Herwig the functional equivalent of a biological father.

680. As a result of the January 8, 2020 Attack and SSG Herwig's injuries, the Plaintiff members of the Herwig Family have experienced severe mental anguish as well as emotional pain and suffering.

681. **Private First Class Brandon Hitchings** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded PFC Hitchings, who suffered from TBI, anxiety, depression, and sleep apnea.

682. Plaintiff PFC Hitchings was a U.S. national at the time of the attack and remains one today.

683. As a result of the January 8, 2020 Attack and his injuries, PFC Hitchings has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

684. **Sergeant Suzanne Hodges** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Hodges, who suffered from TBI, PTSD, anxiety, depression, insomnia, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, and migraines.

685. Plaintiff SGT Hodges was a U.S. national at the time of the attack and remains one today.

686. As a result of the January 8, 2020 Attack and her injuries, SGT Hodges has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

687. **Specialist Kerry Howard** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Howard, who suffered from TBI, PTSD, anxiety, depression, tinnitus, and migraines.

688. Plaintiff SPC Howard was a U.S. national at the time of the attack and remains one today.

689. As a result of the January 8, 2020 Attack and his injuries, SPC Howard has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

690. **Staff Sergeant Andrew Jenkins** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SSG Jenkins, who suffered from TBI, PTSD, sleep apnea, and tinnitus.

691. As a result of the January 8, 2020 Attack and his injuries, SSG Jenkins has experienced severe physical and emotional pain and suffering.

692. Plaintiff SSG Jenkins was a U.S. national at the time of the attack and remains one today.

693. Plaintiff Megan Jenkins is the wife of SSG Jenkins and a U.S. national.

694. Plaintiff A.J., by and through her next friend SSG Jenkins, is the minor daughter of SSG Jenkins. She is a U.S. national.

695. Plaintiff P.J., by and through his next friend SSG Jenkins, is the minor son of SSG Jenkins. He is a U.S. national.

696. Plaintiff S.J., by and through her next friend SSG Jenkins, is the minor daughter of SSG Jenkins. She is a U.S. national.

697. As a result of the January 8, 2020 Attack and SSG Jenkins's injuries, the Plaintiff members of the Jenkins Family have experienced severe mental anguish as well as emotional pain and suffering.

698. **Major Alan Johnson** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded MAJ Johnson, who suffered from TBI, PTSD, insomnia, sleep apnea, eye convergence insufficiency, tinnitus, migraines, cervicgia, cervical lymphadenopathy, and a thyroid nodule.

699. As a result of the January 8, 2020 Attack and his injuries, MAJ Johnson has experienced severe physical and emotional pain and suffering.

700. Plaintiff MAJ Johnson was a U.S. national at the time of the attack and remains one today.

701. Plaintiff Teri Larson-Johnson is the wife of MAJ Johnson and a U.S. national.

702. Plaintiff J.J., by and through his next friend MAJ Johnson, is the minor son of MAJ Johnson. He is a U.S. national.

703. Plaintiff Abby Sigurdson is the stepdaughter of MAJ Johnson and a U.S. national. Ms. Sigurdson lived in the same household as MAJ Johnson for a substantial period and considered MAJ Johnson the functional equivalent of a biological father.

704. Plaintiff Carly Sigurdson is the stepdaughter of MAJ Johnson and a U.S. national. Ms. Sigurdson lived in the same household as MAJ Johnson for a substantial period and considered MAJ Johnson the functional equivalent of a biological father.

705. Plaintiff Samuel Sigurdson is the stepson of Alan Johnson and a U.S. national. Mr. Sigurdson lived in the same household as MAJ Johnson for a substantial period and considered MAJ Johnson the functional equivalent of a biological father.

706. As a result of the January 8, 2020 Attack and MAJ Johnson's injuries, the Plaintiff members of the Johnson Family have experienced severe mental anguish as well as emotional pain and suffering.

707. **Sergeant First Class Brock Johnson** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SFC Johnson, who suffered from PTSD, anxiety, depression, and sleep apnea.

708. As a result of the January 8, 2020 Attack and his injuries, SFC Johnson has experienced severe physical and emotional pain and suffering.

709. Plaintiff SFC Johnson was a U.S. national at the time of the attack and remains one today.

710. Plaintiff Toni Alexander is the wife of SFC Johnson and a U.S. national.

711. As a result of the January 8, 2020 Attack and SFC Johnson's injuries, the Plaintiff members of the Johnson Family have experienced severe mental anguish as well as emotional pain and suffering.

712. **Private First Class Tremayne Joiner** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded PFC Joiner, who suffered from TBI, anxiety, sleep apnea, bilateral vestibular system damage, tinnitus, and migraines.

713. Plaintiff PFC Joiner was a U.S. national at the time of the attack and remains one today.

714. As a result of the January 8, 2020 Attack and his injuries, PFC Joiner has experienced severe mental anguish as well as emotional pain and suffering.

715. **Specialist Robert Jones** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Jones, who suffered from a TBI, PTSD, anxiety, depression, tinnitus, and migraines.

716. Plaintiff SPC Jones was a U.S. national at the time of the attack and remains one today.

717. As a result of the January 8, 2020 Attack and his injuries, SPC Jones has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

718. **Specialist Daunte Keller** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Keller, who suffered from TBI, PTSD, anxiety, depression, and panic disorder.

719. Plaintiff SPC Keller was a U.S. national at the time of the attack and remains one today.

720. As a result of the January 8, 2020 Attack and his injuries, SPC Keller has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

721. **Specialist Alexander Knowles** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Knowles, who suffered from TBI and tinnitus.

722. Plaintiff SPC Alexander Knowles was a U.S. national at the time of the attack and remains one today.

723. As a result of the January 8, 2020 Attack and his injuries, SPC Knowles has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

724. **Sergeant First Class Daine Kvasager** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SFC Kvasager, who suffered from TBI, PTSD, anxiety, depression, insomnia, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, migraines, and autonomic dysfunction.

725. As a result of the January 8, 2020 Attack and his injuries, SFC Kvasager has experienced severe physical and emotional pain and suffering.

726. Plaintiff SFC Kvasager was a U.S. national at the time of the attack and remains one today.

727. Plaintiff C.K., by and through his next friend SFC Kvasager, is the minor son of SFC Kvasager. He is a U.S. national.

728. Plaintiff R.K., by and through his next friend SFC Kvasager, is the minor son of SFC Kvasager. He is a U.S. national.

729. As a result of the January 8, 2020 Attack and SFC Kvasager's injuries, the Plaintiff members of the Kvasager Family have experienced severe mental anguish as well as emotional pain and suffering.

730. **Staff Sergeant Rebecca Kvasager** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SSG Kvasager, who suffered from TBI.

731. As a result of the January 8, 2020 Attack and her injuries, SSG Kvasager has experienced severe physical and emotional pain and suffering.

732. Plaintiff SSG Kvasager was a U.S. national at the time of the attack and remains one today.

733. Plaintiff L.M., by and through her next friend SSG Kvasager, is the minor daughter of SSG Kvasager. She is a U.S. national.

734. As a result of the January 8, 2020 Attack and SSG Kvasager's injuries, the Plaintiff members of the Kvasager Family have experienced severe mental anguish as well as emotional pain and suffering.

735. **Sergeant Kenneth Lewis** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Lewis, who suffered from TBI, PTSD, anxiety, depression, insomnia, sleep apnea, eye convergence insufficiency, tinnitus,

migraines, fibromyalgia, lumber degenerative disc disease, and bilateral radiculopathy in both elbows.

736. As a result of the January 8, 2020 Attack and his injuries, SGT Lewis has experienced severe physical and emotional pain and suffering.

737. Plaintiff SGT Lewis was a U.S. national at the time of the attack and remains one today.

738. Plaintiff Tammy Senecal-Lewis is the wife of SGT Lewis and a U.S. national.

739. Plaintiff K.L., by and through her next friend SGT Lewis, is the minor daughter of SGT Lewis. She is a U.S. national.

740. Plaintiff R.L., by and through his next friend SGT Lewis, is the minor son of SGT Lewis. He is a U.S. national.

741. Plaintiff R.A.L., by and through her next friend SGT Lewis, is the minor daughter of SGT Lewis. She is a U.S. national.

742. Plaintiff TaVera Green is the stepdaughter of SGT Lewis and a U.S. national. Ms. Green lived in the same household as SGT Lewis for a substantial period and considered SGT Lewis the functional equivalent of a biological father.

743. As a result of the January 8, 2020 Attack and SGT Lewis's injuries, the Plaintiff members of the Lewis Family have experienced severe mental anguish as well as emotional pain and suffering.

744. **Sergeant Leighton Lim** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Lim, who suffered from TBI.

745. Plaintiff SGT Lim was a U.S. national at the time of the attack and remains one today.

746. As a result of the January 8, 2020 Attack and his injuries, SGT Lim has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

747. **Staff Sergeant Deanna Lucchesi** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SSG Lucchesi, who suffered from TBI, PTSD, anxiety, depression, insomnia, tinnitus, migraines, benign proximal placement vertigo, and an audio processing disorder.

748. As a result of the January 8, 2020 Attack and her injuries, SSG Lucchesi has experienced severe physical and emotional pain and suffering.

749. Plaintiff SSG Lucchesi was a U.S. national at the time of the attack and remains one today.

750. Plaintiff Joshua Lucchesi is the husband of SSG Lucchesi and a U.S. national.

751. Plaintiff A.L., by and through her next friend SSG Lucchesi, is the minor daughter of SSG Lucchesi. She is a U.S. national.

752. Plaintiff H.L., by and through her next friend SSG Lucchesi, is the minor daughter of SSG Lucchesi. She is a U.S. national.

753. Plaintiff Z.L., by and through her next friend SSG Lucchesi, is the minor daughter of SSG Lucchesi. She is a U.S. national.

754. As a result of the January 8, 2020 Attack and SSG Lucchesi's injuries, the Plaintiff members of the Lucchesi Family have experienced severe mental anguish as well as emotional pain and suffering.

755. **Sergeant John Magee** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Magee, who suffered from PTSD

and severe TBI symptoms including headaches, tinnitus, and medically documented sleep problems.

756. Plaintiff SGT Magee was a U.S. national at the time of the attack and remains one today.

757. As a result of the January 8, 2020 Attack and his injuries, SGT Magee has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

758. **Sergeant Darius Martin** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Martin, who suffered from TBI, PTSD, anxiety, depression, insomnia, sleep apnea, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, and migraines.

759. As a result of the January 8, 2020 Attack and his injuries, SGT Martin has experienced severe physical and emotional pain and suffering.

760. Plaintiff SGT Martin was a U.S. national at the time of the attack and remains one today.

761. Plaintiff Amanda Martin is the wife of SGT Martin and a U.S. national.

762. Plaintiff M.M., by and through his next friend SGT Martin, is the minor son of SGT Martin. He is a U.S. national.

763. Plaintiff Darlina Martin is the mother of SGT Martin and a U.S. national.

764. Plaintiff Cayleigh Martin is the sister of SGT Martin and a U.S. national.

765. As a result of the January 8, 2020 Attack and SGT Martin's injuries, the Plaintiff members of the Martin Family have experienced severe mental anguish as well as emotional pain and suffering.

766. **Specialist Isaac Martz** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Martz, who suffered from TBI, PTSD, depression, and insomnia.

767. Plaintiff SPC Martz was a U.S. national at the time of the attack and remains one today.

768. As a result of the January 8, 2020 Attack and his injuries SPC Martz has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

769. **Staff Sergeant Torrin Mcdougale** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SSG Mcdougale, who suffered from TBI.

770. Plaintiff SSG Mcdougale was a U.S. national at the time of the attack and remains one today.

771. As a result of the January 8, 2020 Attack and his injuries, SSG Mcdougale has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

772. **Sergeant Phillip Mendoza** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Mendoza, who suffered from TBI, PTSD, anxiety, depression, sleep apnea, and migraines.

773. As a result of the January 8, 2020 Attack and his injuries, SGT Mendoza has experienced severe physical and emotional pain and suffering.

774. Plaintiff SGT Mendoza was a U.S. national at the time of the attack and remains one today.

775. Plaintiff Melchi Mendoza is the wife of SGT Mendoza and a U.S. national.

776. Plaintiff A.M., by and through his next friend SGT Mendoza, is the minor son of SGT Mendoza. He is a U.S. national.

777. As a result of the January 8, 2020 Attack and SGT Mendoza's injuries, the Plaintiff members of the Mendoza Family have experienced severe mental anguish as well as emotional pain and suffering.

778. **Sergeant Zachary Merrill** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Merrill, who suffered from TBI, PTSD, anxiety, sleep apnea, tinnitus, and tension headaches.

779. As a result of the January 8, 2020 Attack and his injuries, SGT Merrill has experienced severe physical and emotional pain and suffering.

780. Plaintiff SGT Merrill was a U.S. national at the time of the attack and remains one today.

781. Plaintiff Carolina Merrill is the wife of SGT Merrill and a U.S. national.

782. Plaintiff C.M., by and through her next friend SGT Merrill, is the minor daughter of SGT Merrill. She is a U.S. national.

783. As a result of the January 8, 2020 Attack and SGT Merrill's injuries, the Plaintiff members of the Merrill Family have experienced severe mental anguish as well as emotional pain and suffering.

784. **Sergeant James Morgan** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Morgan, who suffered from TBI, PTSD, tinnitus, and migraines.

785. As a result of the January 8, 2020 Attack and his injuries, SGT Morgan has experienced severe physical and emotional pain and suffering.

786. Plaintiff SGT Morgan was a U.S. national at the time of the attack and remains one today.

787. Plaintiff Sarah Morgan is the wife of SGT Morgan and a U.S. national.

788. Plaintiff C.M., by and through her next friend SGT Morgan, is the minor daughter of SGT Morgan. She is a U.S. national.

789. As a result of the January 8, 2020 Attack and SGT Morgan's injuries, the Plaintiff members of the Morgan Family have experienced severe mental anguish as well as emotional pain and suffering.

790. **Specialist Ryan Nolan** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Nolan, who suffered from TBI and a lower back injury.

791. Plaintiff SPC Nolan was a U.S. national at the time of the attack and remains one today.

792. As a result of the January 8, 2020 Attack and his injuries, SPC Nolan has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

793. **Sergeant Brittany Norfleet** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Norfleet, who suffered from TBI, PTSD, anxiety, depression, insomnia, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, and migraines.

794. As a result of the January 8, 2020 Attack and her injuries, SGT Norfleet has experienced severe physical and emotional pain and suffering.

795. Plaintiff SGT Norfleet was a U.S. national at the time of the attack and remains one today.

796. Plaintiff Anthony Shappy is the husband of SGT Norfleet and a U.S. national.

797. Plaintiff A.S., by and through her next friend SGT Norfleet, is the minor daughter of SGT Norfleet. She is a U.S. national.

798. Plaintiff K.S., by and through her next friend SGT Norfleet, is the minor daughter of SGT Norfleet. She is a U.S. national.

799. As a result of the January 8, 2020 Attack and SGT Norfleet's injuries, the Plaintiff members of the Norfleet Family have experienced severe mental anguish as well as emotional pain and suffering.

800. **Specialist Jose Ortiz** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Ortiz, who suffered from TBI.

801. Plaintiff SPC Ortiz was a U.S. national at the time of the attack and remains one today.

802. As a result of the January 8, 2020 Attack and his injuries, SPC Ortiz has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

803. **Sergeant Anthony Panchoo** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Panchoo, who suffered from TBI, depression, sleep apnea, and migraines.

804. As a result of the January 8, 2020 Attack and his injuries, SGT Panchoo has experienced severe physical and emotional pain and suffering.

805. Plaintiff SGT Panchoo was a U.S. national at the time of the attack and remains one today.

806. Plaintiff Alexis Panchoo is the wife of SGT Panchoo and a U.S. national.

807. Plaintiff A.P., by and through her next friend SGT Panchoo, is the minor daughter of SGT Panchoo. She is a U.S. national.

808. As a result of the January 8, 2020 Attack and SGT Panchoo's injuries, the Plaintiff members of the Panchoo Family have experienced severe mental anguish as well as emotional pain and suffering.

809. **Sergeant First Class Carlos Porres Jr.** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SFC Porres, who suffered from TBI, anxiety, depression, insomnia, and sleep apnea.

810. As a result of the January 8, 2020 Attack and his injuries, SFC Porres has experienced severe physical and emotional pain and suffering.

811. Plaintiff SFC Porres was a U.S. national at the time of the attack and remains one today.

812. Plaintiff K.L.P., by and through her next friend SFC Porres, is the minor daughter of SFC Porres. She is a U.S. national.

813. Plaintiff K.R.P., by and through her next friend SFC Porres, is the minor daughter of SFC Porres. She is a U.S. national.

814. As a result of the January 8, 2020 Attack and SFC Porres's injuries, the Plaintiff members of the Porres Family have experienced severe mental anguish as well as emotional pain and suffering.

815. **Chief Warrant Officer 2 Michael Pridgeon** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded CW2 Pridgeon, who suffered from TBI, PTSD, sleep apnea, tinnitus, and migraines.

816. As a result of the January 8, 2020 Attack and his injuries, CW2 Pridgeon has experienced severe physical and emotional pain and suffering.

817. Plaintiff CW2 Pridgeon was a U.S. national at the time of the attack and remains one today.

818. Plaintiff Rebecca Pridgeon is the wife of CW2 Pridgeon and a U.S. national.

819. Plaintiff A.P., by and through her next friend CW2 Pridgeon, is the minor daughter of CW2 Pridgeon. She is a U.S. national.

820. Plaintiff M.P., by and through his next friend CW2 Pridgeon, is the minor son of CW2 Pridgeon. He is a U.S. national.

821. Plaintiff T.P., by and through his next friend CW2 Pridgeon, is the minor son of CW2 Pridgeon. He is a U.S. national.

822. As a result of the January 8, 2020 Attack and CW2 Pridgeon's injuries, the Plaintiff members of the Pridgeon Family have experienced severe mental anguish as well as emotional pain and suffering.

823. **Technical Sergeant Rachel Quinn** served in Iraq as a member of the U.S. Air Force at the time of the attack. The January 8, 2020 Attack severely wounded TSgt Quinn, who suffered from TBI, PTSD, anxiety, depression, panic disorder, insomnia, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, migraines, psoriasis, and psoriatic arthritis.

824. Plaintiff TSgt Quinn was a U.S. national at the time of the attack and remains one today.

825. As a result of the January 8, 2020 Attack and her injuries TSgt Quinn has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

826. **Sergeant Jason Quitugua II** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Quitugua, who suffered from TBI and PTSD.

827. As a result of the January 8, 2020 Attack and his injuries, SGT Quitugua experienced severe physical and emotional pain and suffering. SGT Quitugua died on October 7, 2021 by suicide.

828. SGT Quitugua was a U.S. national at the time of the attack and his death.

829. Plaintiff Francine Rios is the mother of SGT Quitugua and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of SGT Quitugua's estate.

830. Plaintiff Mckenzie-Jae Quitugua is the sister of SGT Quitugua and a U.S. national.

831. Plaintiff Kaedinn Quitugua is the sister of SGT Quitugua and a U.S. national.

832. Plaintiff Summer Quitugua is the sister of SGT Quitugua and a U.S. national.

833. As a result of the January 8, 2020 Attack and SGT Quitugua's injuries, the Plaintiff members of the Quitugua Family have experienced severe mental anguish as well as emotional pain and suffering, and the loss of SGT Quitugua's society, companionship, and counsel.

834. As a result of the January 8, 2020 Attack, SGT Quitugua was injured in his person and/or property. The Plaintiff members of the Quitugua Family are the survivors and/or heirs of SGT Quitugua and are entitled to recover for the damages SGT Quitugua sustained.

835. **Specialist Nilsa Rivera Villegas** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Rivera Villegas, who suffered from TBI and PTSD.

836. Plaintiff SPC Rivera Villegas was a U.S. national at the time of the attack and remains one today.

837. As a result of the January 8, 2020 Attack and her injuries, SPC Rivera Villegas has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

838. **Staff Sergeant Jacob Schmidt** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SSG Schmidt, who suffered from TBI.

839. Plaintiff SSG Schmidt was a U.S. national at the time of the attack and remains one today.

840. As a result of the January 8, 2020 Attack and his injuries, SSG Schmidt has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

841. **Private First Class Jaron Schneider** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded PFC Schneider, who suffered from TBI, PTSD, anxiety, depression, sleep apnea, eye convergence insufficiency, bilateral vestibular system damage, tinnitus, and migraines.

842. As a result of the January 8, 2020 Attack and his injuries, PFC Schneider has experienced severe physical and emotional pain and suffering.

843. Plaintiff PFC Schneider was a U.S. national at the time of the attack and remains one today.

844. Plaintiff Ashley Schneider is the wife of PFC Schneider and a U.S. national.

845. As a result of the January 8, 2020 Attack and PFC Schneider's injuries, the Plaintiff members of the Schneider Family have experienced severe mental anguish as well as emotional pain and suffering.

846. **Private First Class Collin Shepard** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded PFC Shepard, who suffered from TBI and anxiety.

847. As a result of the January 8, 2020 Attack and his injuries, PFC Shepard has experienced severe physical and emotional pain and suffering.

848. Plaintiff PFC Shepard was a U.S. national at the time of the attack and remains one today.

849. Plaintiff Kaitlin Shepard is the wife of PFC Shepard and a U.S. national.

850. As a result of the January 8, 2020 Attack and PFC Shepard's injuries, the Plaintiff members of the Shepard Family have experienced severe mental anguish as well as emotional pain and suffering.

851. **Sergeant Frederick Shilke** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Shilke, who suffered from TBI, PTSD, anxiety, depression, panic disorder, and insomnia.

852. As a result of the January 8, 2020 Attack and his injuries, SGT Shilke has experienced severe physical and emotional pain and suffering.

853. Plaintiff SGT Shilke was a U.S. national at the time of the attack and remains one today.

854. Plaintiff Stephanie Shilke is the wife of SGT Shilke and a U.S. national.

855. Plaintiff W.S., by and through his next friend SGT Shilke, is the minor son of SGT Shilke. He is a U.S. national.

856. Plaintiff M.C.R., by and through his next friend Stephanie Shilke, is the minor stepson of SGT Shilke and is a U.S. national. M.C.R. lived in the same household as SGT Shilke for a substantial period and considered SGT Shilke the functional equivalent of a biological father.

857. Plaintiff M.D.R., by and through her next friend Stephanie Shilke, is the minor stepdaughter of SGT Shilke and is a U.S. national. M.D.R. lived in the same household as SGT Shilke for a substantial period and considered SGT Shilke the functional equivalent of a biological father.

858. As a result of the January 8, 2020 Attack and SGT Shilke's injuries, the Plaintiff members of the Shilke Family have experienced severe mental anguish as well as emotional pain and suffering.

859. **Private First Class Michael Smith** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded PFC Smith, who suffered from TBI, PTSD, anxiety, depression, and tinnitus.

860. As a result of the January 8, 2020 Attack and his injuries, PFC Smith has experienced severe physical and emotional pain and suffering.

861. Plaintiff PFC Smith was a U.S. national at the time of the attack and remains one today.

862. Plaintiff Corisia Smith is the wife of PFC Smith and a U.S. national.

863. Plaintiff A.S., by and through her next friend PFC Smith, is the minor daughter of PFC Smith. She is a U.S. national.

864. Plaintiff A.D., by and through her next friend Corisia Smith, is the minor stepdaughter of PFC Smith and is a U.S. national. A.D. lived in the same household as PFC Smith for a substantial period and considered PFC Smith the functional equivalent of a biological father.

865. As a result of the January 8, 2020 Attack and PFC Smith's injuries, the Plaintiff members of the Smith Family have experienced severe mental anguish as well as emotional pain and suffering.

866. **Specialist Gregory Sorensen** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Sorensen, who suffered from TBI, PTSD, and anxiety.

867. Plaintiff SPC Sorensen was a U.S. national at the time of the attack and remains one today.

868. As a result of the January 8, 2020 Attack and his injuries, SPC Sorensen has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

869. **Hugh Spears Jr.** was in Iraq as a civilian contractor working for KBR at the time of the attack. The January 8, 2020 Attack severely wounded Hugh Spears, who suffered from an existing lower back injury which was exacerbated by the attack and is now medicated for severe PTSD which includes sleep issues, anxiety, and flashbacks.

870. As a result of the January 8, 2020 Attack and his injuries, Hugh Spears has experienced severe physical and emotional pain and suffering.

871. Plaintiff Hugh Spears was a U.S. national at the time of the attack and remains one today.

872. Plaintiff Brandon Spears is the son of Hugh Spears and a U.S. national.

873. As a result of the January 8, 2020 Attack and Hugh Spears's injuries the Plaintiff members of the Spears Family have experienced severe mental anguish as well as emotional pain and suffering.

874. **Specialist Johnathan Stark** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Stark, who suffered from TBI, PTSD, anxiety, and insomnia.

875. Plaintiff SPC Stark was a U.S. national at the time of the attack and remains one today.

876. As a result of the January 8, 2020 Attack and his injuries, SPC Stark has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

877. **William Taber** was working in Iraq as a civilian contractor for the Department of the Army at the time of the attack. The January 8, 2020 Attack severely wounded William Taber, who suffered from TBI, PTSD, anxiety, depression, insomnia, sleep apnea, tinnitus, and migraines.

878. As a result of the January 8, 2020 Attack and his injuries, William Taber has experienced severe physical and emotional pain and suffering.

879. Plaintiff William Taber was a U.S. national at the time of the attack and remains one today.

880. Plaintiff Dagmar Taber is the wife of William Taber and a German citizen.

881. Plaintiff Louis Palla is the son of William Taber and a German citizen.

882. Plaintiff Samira Palla is the daughter of William Taber and a German citizen.

883. Plaintiff A.T., by and through her next friend William Taber, is the minor daughter of William Taber. She is a U.S. national.

884. As a result of the January 8, 2020 Attack and William Taber's injuries, the Plaintiff members of the Taber family have experienced severe mental anguish as well as emotional pain and suffering.

885. **Specialist Nicolaus Trivelpiece** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Trivelpiece, who suffered from TBI and migraines.

886. Plaintiff SPC Trivelpiece was a U.S. national at the time of the attack and remains one today.

887. As a result of the January 8, 2020 Attack and his injuries, SPC Trivelpiece has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

888. **Staff Sergeant Sandro Vicente** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SSG Vicente, who suffered from TBI, anxiety, depression, sleep apnea, and other PTSD-related symptoms.

889. Plaintiff SSG Vicente was a U.S. national at the time of the attack and remains one today.

890. As a result of the January 8, 2020 Attack and his injuries, SSG Vicente has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

891. **Specialist Luis Villegas** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Villegas, who suffered from TBI.

892. Plaintiff SPC Villegas was a U.S. national at the time of the attack and remains one today.

893. As a result of the January 8, 2020 Attack and his injuries, SPC Villegas has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

894. **First Lieutenant Hailey Webster** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded 1LT Webster, who suffered from TBI, PTSD, anxiety, depression, eye convergence insufficiency, tinnitus, migraines, temporomandibular joint disorder, increased allergies, neck pain, and constant tense muscles.

895. As a result of the January 8, 2020 Attack and her injuries, 1LT Webster has experienced severe physical and emotional pain and suffering.

896. Plaintiff 1LT Webster was a U.S. national at the time of the attack and remains one today.

897. Plaintiff John Goetz is the husband of 1LT Webster and a U.S. national.

898. As a result of the January 8, 2020 Attack and 1LT Webster's injuries, the Plaintiff members of the Webster Family have experienced severe mental anguish as well as emotional pain and suffering.

899. **Sergeant Jeremy Winkler** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SGT Winkler, who suffered from TBI, PTSD, anxiety, depression, insomnia, sleep apnea, tinnitus, and migraines.

900. As a result of the January 8, 2020 Attack and his injuries, SGT Winkler has experienced severe physical and emotional pain and suffering.

901. Plaintiff SGT Winkler was a U.S. national at the time of the attack and remains one today.

902. Plaintiff Tyla Winkler is the wife of SGT Winkler and a U.S. national.

903. Plaintiff M.A.W., by and through his next friend SGT Winkler, is the minor son of SGT Winkler. He is a U.S. national.

904. Plaintiff M.I.W., by and through his next friend SGT Winkler, is the minor son of SGT Winkler. He is a U.S. national.

905. Plaintiff M.Z.W., by and through her next friend SGT Winkler, is the minor daughter of SGT Winkler. She is a U.S. national.

906. As a result of the January 8, 2020 Attack and SGT Winkler's injuries, the Plaintiff members of the Winkler Family have experienced severe mental anguish as well as emotional pain and suffering.

907. **Specialist Mason Wright** served in Iraq as a member of the U.S. Army at the time of the attack. The January 8, 2020 Attack severely wounded SPC Wright, who suffered from TBI, PTSD, anxiety, depression, sleep apnea, tinnitus, and migraines.

908. As a result of the January 8, 2020 Attack and his injuries, SPC Wright has experienced severe physical and emotional pain and suffering.

909. Plaintiff SPC Wright was a U.S. national at the time of the attack and remains one today.

910. Plaintiff A.V., by and through her next friend SPC Wright, is the minor daughter of SPC Wright. She is a U.S. national.

911. As a result of the January 8, 2020 Attack and SPC Wright's injuries, the Plaintiff members of the Wright Family have experienced severe mental anguish as well as emotional pain and suffering.

#### **4. The March 11, 2020 Rocket Attack in Iraq (Covarrubias Family)**

912. On March 11, 2020, a joint cell comprised of Hezbollah and Kataib Hezbollah, for which the IRGC, including IRGC-QF and IRGC-IO, provided funding, training, weapons,

logistical support, and intelligence, committed a rocket attack in Baghdad, Iraq (the “March 11, 2020 Attack”).

913. The March 11, 2020 Attack was planned and authorized by, *inter alia*, Hezbollah, the IRGC-QF, and Kataib Hezbollah.

914. The March 11, 2020 Attack was aided by IRGC-funded and supplied bounty payments and martyr payments to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; both types of payments were designed to, and did, incentivize Hezbollah’s and Kataib Hezbollah’s successful attacks, including the March 11, 2020 Attack.

915. The March 11, 2020 Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made rockets, rocket launchers, artillery computer systems, optics, drones, and satellite imagery, which the IRGC (through the IRGC-QF and the IRGC-IO) made available to Hezbollah and Kataib Hezbollah.

916. The March 11, 2020 Attack relied upon IRGC-supplied intelligence, including, but not limited to, intelligence from IRGC-supplied drones and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah, as well as Hezbollah’s and Kataib Hezbollah’s terrorists on the ground in Baghdad, who served as the IRGC’s, Hezbollah’s, and Kataib Hezbollah’s intelligence eyes and ears in the area.

917. The March 11, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

918. The March 11, 2020 Attack furthered the Axis Conspiracy by demonstrating the IRGC’s (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly

threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by March 11, 2020 Attack given its high-profile nature.

919. **Specialist Juan Covarrubias** served in Iraq as a member of the U.S. Army. SPC Covarrubias was injured in the March 11, 2020 Attack. SPC Covarrubias died on March 11, 2020, as a result of injuries sustained during the attack.

920. SPC Covarrubias was a U.S. national at the time of the attack and his death.

921. Plaintiff Bianca Meza-Covarrubias is the widow of SPC Covarrubias and a U.S. national.

922. As a result of the March 11, 2020 Attack and SPC Covarrubias's injuries and death, Plaintiff Bianca Meza-Covarrubias has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Covarrubias's society, companionship, and counsel.

923. As a result of the March 11, 2020 Attack, SPC Covarrubias was injured in his person and/or property. Plaintiff Bianca Meza-Covarrubias is the survivor and/or heir of SPC Covarrubias and is entitled to recover for the damages SPC Covarrubias sustained.

## 5. **The September 28, 2022 Rocket and Drone Attack in Iraq (Mahmoudzadeh Family)**

924. On September 28, 2022, a joint cell comprised of Hezbollah and Kataib Hezbollah (in Iraqi Kurdistan) and the IRGC (in Iran), committed a rocket and UAV attack in Kurdistan, Iraq (the "September 28, 2022 Attack").

925. The September 28, 2022 Attack was planned and authorized by the IRGC.

926. The September 28, 2022 Attack was aided by IRGC-funded and supplied bounty payments and martyr payments to operatives from the IRGC, Hezbollah, and Kataib Hezbollah; both types of payments were designed to, and did, incentivize Hezbollah's and Kataib Hezbollah's successful attacks, including the September 28, 2022 Attack.

927. The September 28, 2022 Attack relied upon IRGC-supplied weapons, including, but not limited to, IRGC-made rockets, rocket launchers, artillery computer systems, optics, drones, and satellite imagery, which the IRGC (through the IRGC-QF and the IRGC-IO) made available to Hezbollah and Kataib Hezbollah.

928. The September 28, 2022 Attack relied upon IRGC-supplied intelligence, including, but not limited to, intelligence from IRGC-supplied drones and satellite imagery, which the IRGC gave to Hezbollah and Kataib Hezbollah, as well as Hezbollah's and Kataib Hezbollah's terrorists on the ground in Iraqi Kurdistan, who served as the IRGC's, Hezbollah's, and Kataib Hezbollah's intelligence eyes and ears in the area.

929. The September 28, 2022 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

930. The September 28, 2022 Attack furthered the Axis Conspiracy by demonstrating the IRGC's (through IRGC proxies Hezbollah and Kataib Hezbollah) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to

collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by September 28, 2022 Attack given its high-profile nature.

931. **Omer Mahmoudzadeh** was in Iraq helping refugees in camps near the Democratic Party of Iranian Kurdistan ("KDP-I") headquarters at the time of the attack. Omer Mahmoudzadeh was injured in the September 28, 2022 Attack. Omer Mahmoudzadeh died on September 28, 2022, as a result of injuries sustained during the attack.

932. Omer Mahmoudzadeh was a U.S. national at the time of the attack and his death.

933. Plaintiff Shiwa Nahadi is the widow of Omer Mahmoudzadeh and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Omer Mahmoudzadeh's estate.

934. Plaintiff Tara Mahmoudzadeh is the daughter of Omer Mahmoudzadeh and a U.S. national.

935. As a result of the September 28, 2022 Attack and Omer Mahmoudzadeh's injuries and death, each member of the Mahmoudzadeh Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Omer Mahmoudzadeh's society, companionship, and counsel.

936. As a result of the September 28, 2022 Attack, Omer Mahmoudzadeh was injured in his person and/or property. The Plaintiff members of the Mahmoudzadeh Family are the survivors and/or heirs of Omer Mahmoudzadeh and are entitled to recover for the damages Omer Mahmoudzadeh sustained.

**B. The IRGC-Sponsored Attacks by Hezbollah, Hamas, and PIJ in Israel**

**1. The October 7, 2023 Attack in Israel (Brauner and Gabay)**

937. On October 7, 2023, Hamas and PIJ jointly committed a complex multi-front mass terrorist attack targeting dozens of sites in Israel, which attack included a bomb attack in Tel Aviv, Israel (the “October 7, 2023 Attack”).

938. The October 7, 2023 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victims of this attack were civilians not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

939. The October 7, 2023 Attack furthered the Axis Conspiracy by, *inter alia*: (1) supplying co-Conspirator Hamas with hostages whom the IRGC, Hamas, Binance, and Zhao could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC’s continuing ability (through IRGC proxies Hamas and PIJ) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC’s, Binance’s, and Zhao’s ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC’s ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the October 7, 2023 Attack given its high-profile nature.

940. **Bernadette Brauner** was in Israel visiting her husband’s family at the time of the attack. The October 7, 2023 Attack severely wounded Bernadette Brauner, who suffered from severe PTSD, often having flashbacks of being in a sweltering bomb shelter for over twenty hours.

941. As a result of the October 7, 2023 Attack and her injuries, Bernadette Brauner has experienced severe physical and emotional pain and suffering.

942. Plaintiff Bernadette Brauner was a U.S. national at the time of the attack and remains one today.

943. Plaintiff Nir Brauner is the husband of Bernadette Brauner and a U.S. national.

944. As a result of the October 7, 2023 Attack and Bernadette Brauner's injuries, the Plaintiff members of the Brauner family have experienced severe mental anguish as well as emotional pain and suffering.

945. **Nir Brauner** was in Israel visiting his family at the time of the attack. The October 7, 2023 Attack severely wounded Nir Brauner, who suffered from severe PTSD, often having flashbacks of being in a sweltering bomb shelter for over twenty hours.

946. As a result of the October 7, 2023 Attack and his injuries, Nir Brauner has experienced severe physical and emotional pain and suffering.

947. Plaintiff Nir Brauner was a U.S. national at the time of the attack and remains one today.

948. Plaintiff Bernadette Brauner is the wife of Nir Brauner and a U.S. national.

949. As a result of the October 7, 2023 Attack and Nir Brauner's injuries, the Plaintiff members of the Brauner family have experienced severe mental anguish as well as emotional pain and suffering.

950. **Sheerel Gabay** was in Israel attending the Supernova music festival with friends at the time of the attack. Sheerel Gabay hid with over 30 other people in a roadside bomb shelter near Be'eri, where for more than seven hours, Hamas lobbed grenades and fired at the people inside. Sheerel Gabay was trapped under the lifeless body of a woman who was shot. The

October 7, 2023 Attack severely wounded Sheerel Gabay, who suffered from a gunshot wound to the knee, two open fractures, and a ruptured eardrum.

951. Plaintiff Sheerel Gabay was a U.S. national at the time of the attack and remains one today.

952. As a result of the October 7, 2023 Attack and her, Sheerel Gabay has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

**C. The IRGC's Hostage Taking Attacks in Iran and the United States**

**1. The August 2019 Hostage-Taking Campaign in the United States (Amir Fakhravar)**

953. Since at least in or around August 2019, the IRGC has perpetrated an ongoing campaign of attempting to take Plaintiff **Amir Fakhravar** hostage from the United States, render him to Iran, force him to confess to crimes against the Islamic Republic of Iran, and then murder him (the “Attack Campaign”). The Attack Campaign has involved repeated, failed attempts by IRGC agents to kidnap Amir Fakhravar, and sophisticated efforts to promote other violent acts, including by inspiring an IRGC lone-wolf terrorist in the United States to kidnap or murder him.

954. To terrorize Amir Fakhravar, the IRGC devised the Attack Campaign, which involved a litany of violent acts that the IRGC pursued with the specific intent to terrorize Amir Fakhravar and, among other things, cause him to die by suicide or of natural causes brought on by the IRGC's campaign of unrelenting terror, e.g., having a heart attack.

955. To terrorize Amir Fakhravar (and other regime enemies similarly situated), the IRGC conducted acts of international terrorism against persons in the United States and Europe who were closely associated with Amir Fakhravar or, alternatively, in the same category of “regime enemy” as Amir Fakhravar. With respect to the latter, the IRGC has directly threatened

Amir Fakhravar on IRGC-controlled media outlets and, in effect, called for his murder by any pious Shiite Muslim who can locate Amir anywhere in the world.

956. Amir Fakhravar was a writer, journalist, and U.S. national at the time of the attack and remains one today. The Attack Campaign severely wounded Amir Fakhravar, who suffered psychological trauma and mental anguish from IRGC's campaign to take him hostage.

957. Plaintiff Amir Fakhravar is a U.S. national.

958. The Attack Campaign would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

959. The Attack Campaign furthered the Axis Conspiracy by demonstrating the IRGC's continuing ability to credibly threaten to commit an act of terrorism anywhere in the world, even against someone in residing at an undisclosed location in the United States, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for credibly threatening violence, which was bolstered by the Attack Campaign given its high-profile nature.

960. As a result of the Attack Campaign and his injuries, Amir Fakhravar has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

## **2. The September 28, 2019 Hostage-Taking Attack in Iran (Akbar Lakestani)**

961. On September 28, 2019, the IRGC committed a hostage-taking attack in Tehran, Iran (the "September 28, 2019 Attack").

962. The September 28, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

963. The September 28, 2019 Attack furthered the Axis Conspiracy by, *inter alia*: (1) supplying the IRGC with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the September 28, 2019 Attack given its high-profile nature.

964. **Akbar Lakestani** was in Iran visiting his sick and elderly mother at the time of the attack. The September 28, 2019 Attack severely wounded Akbar Lakestani, who was held hostage by the IRGC for nearly 6 months, and continues to suffer from PTSD.

965. Plaintiff Akbar Lakestani was a U.S. national at the time of the attack and remains one today.

966. As a result of the September 28, 2019 Attack and his injuries, Akbar Lakestani has experienced severe mental anguish as well as severe physical and emotional pain and suffering.

**D. The IRGC-Sponsored Attacks by Al-Qaeda in Afghanistan and Kenya**

**1. The August 7, 2016 Hostage-Taking and Torture in Afghanistan (King Family)**

967. On August 7, 2016, a joint cell comprised of FTOs, al-Qaeda and the Haqqani Network, committed a hostage-taking attack at gunpoint in Kabul, Afghanistan (the “August 7, 2016 Attack”). Al-Qaeda planned, authorized, and financially supported the attack and subsequent detention and torture of the hostage.

968. The August 7, 2016 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

969. The August 7, 2016 Attack furthered the Axis Conspiracy by, *inter alia*: (1) supplying co-Conspirators al-Qaeda and the Taliban (including its Haqqani Network) with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC’s continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC’s, Binance’s, and Zhao’s ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC’s ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the August 7, 2016 Attack given its high-profile nature.

970. **Kevin King** was in Afghanistan as a civilian professor teaching at American University of Afghanistan at the time of the attack. The August 7, 2016 Attack severely wounded

Kevin King, who was held captive for 39 months (over 3 years). He suffered from severe caloric malnutrition, muscle atrophy, peripheral neuropathy, hypocalcemia, vitamin D deficiency, low bone mineral density, elevated PTH (hyperparathyroidism), and frostbite on feet and ankles. He also suffered from a weak bladder and an umbilical hernia, which is likely due to the repeated beatings he endured.

971. As a result of the August 7, 2016 Attack and his injuries, Kevin King has experienced severe physical and emotional pain and suffering.

972. Plaintiff Kevin King was a U.S. national at the time of the attack and remains one today.

973. Plaintiff Stephanie Miller is the sister of Kevin King and a U.S. national.

974. As a result of the August 7, 2016 Attack and Kevin King's injuries, the Plaintiff members of the King Family have experienced severe mental anguish as well as emotional pain and suffering.

## **2. The January 14, 2019 Suicide Bombing Attack in Afghanistan (Kamaleson Family)**

975. On January 14, 2019, a joint cell comprised of an FTO, al-Qaeda, and the Taliban, acting together as the Kabul Attack Network, committed a suicide bombing attack in Kabul, Afghanistan (the "January 14, 2019 Attack").

976. The January 14, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

977. The January 14, 2019 Attack furthered the Axis Conspiracy by demonstrating the IRGC's continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the January 14, 2019 Attack given its high-profile nature.

978. **Manoharan Kamaleson** was in Afghanistan as the chief operating officer with First MicroFinance Bank at the time of the attack. Manoharan Kamaleson was injured in the January 14, 2019 Attack. Manoharan Kamaleson died on January 14, 2019, as a result of injuries sustained during the attack.

979. Manoharan Kamaleson was a U.S. national at the time of the attack and his death.

980. Plaintiff Nicole Kamaleson is the widow of Manoharan Kamaleson and a U.S. national.

981. Plaintiff Barclay Kamaleson is the son of Manoharan Kamaleson and a U.S. national.

982. Plaintiff Cade Kamaleson is the son of Manoharan Kamaleson and a U.S. national.

983. Plaintiff Cedric Kamaleson is the son of Manoharan Kamaleson and a U.S. national.

984. Plaintiff Sunderraj Kamaleson is the brother of Manoharan Kamaleson and a U.S. national.

985. As a result of the January 14, 2019 Attack and Manoharan Kamaleson's injuries and death, each member of the Kamaleson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Manoharan Kamaleson's society, companionship, and counsel.

986. As a result of the January 14, 2019 Attack, Manoharan Kamaleson was injured in his person and/or property. The Plaintiff members of the Kamaleson Family are the survivors and/or heirs of Manoharan Kamaleson and are entitled to recover for the damages Manoharan Kamaleson sustained.

### **3. The July 13, 2019 Small Arms Attack in Afghanistan (Sartor Family)**

987. On July 13, 2019, a joint cell comprised of al-Qaeda and the Taliban, as directly assisted by the IRGC, including the IRGC's Qods Force, combined together to commit a small arms fire attack in Faryab, Afghanistan (the "July 13, 2019 Attack").

988. The July 13, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

989. The July 13, 2019 Attack furthered the Axis Conspiracy by demonstrating the IRGC's (through IRGC proxies al-Qaeda and the Taliban) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 13, 2019 Attack given its high-profile nature.

990. **Sergeant Major James Sartor** served in Afghanistan as a member of the U.S. Army. SGM Sartor was injured in the July 13, 2019 Attack. SGM Sartor died on July 13, 2019, as a result of injuries sustained during the attack.

991. SGM Sartor was a U.S. national at the time of the attack and his death.

992. Plaintiff Deanna Sartor is the widow of SGM Sartor and a U.S. national.

993. Plaintiff G.S., by and through his next friend Deanna Sartor, is the minor son of SGM Sartor. He is a U.S. national.

994. Plaintiff Grace Sartor is the daughter of SGM Sartor and a U.S. national.

995. Plaintiff Stryder Sartor is the son of SGM Sartor and a U.S. national.

996. Plaintiff Mary Pryor-Patterson is the mother of SGM Sartor and a U.S. national.

997. Plaintiff James Sartor is the father of SGM Sartor and a U.S. national.

998. Plaintiff Shae Sartor is the sister of SGM Sartor and a U.S. national.

999. As a result of the July 13, 2019 Attack and SGM Sartor's injuries and death, each member of the Sartor Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGM Sartor's society, companionship, and counsel.

1000. As a result of the July 13, 2019 Attack, SGM Sartor was injured in his person and/or property. The Plaintiff members of the Sartor Family are the survivors and/or heirs of SGM Sartor and are entitled to recover for the damages SGM Sartor sustained.

**4. The July 29, 2019 Insider Attack in Afghanistan (Kreischer and Nance Families)**

1001. On July 29, 2019, the Taliban, including its Haqqani Network, committed an insider attack involving small arms fire against U.S. Army personnel in Kandahar, Afghanistan (the "July 29, 2019 Attack"). On information and belief, al-Qaeda/Taliban polyterrorist

Sirajuddin Haqqani personally planned the insider attack campaign that included this attack, and therefore, the attack was also directly planned by al-Qaeda.

1002. The July 29, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1003. The July 29, 2019 Attack furthered the Axis Conspiracy by demonstrating the IRGC's (through IRGC proxies al-Qaeda and the Taliban) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's, and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the July 29, 2019 Attack given its high-profile nature.

1004. **Private First Class Brandon Kreischer** served in Afghanistan as a member of the U.S. Army. PFC Kreischer was injured in the July 29, 2019 Attack. PFC Kreischer died on July 29, 2019, as a result of injuries sustained during the attack.

1005. PFC Kreischer was a U.S. national at the time of the attack and his death.

1006. Plaintiff Grace Kreischer is the widow of PFC Kreischer and a U.S. national.

1007. Plaintiff C.K., by and through his next friend Grace Kreischer, is the minor son of PFC Kreischer. He is a U.S. national.

1008. Plaintiff Brianne Barlow is the mother of PFC Kreischer and a U.S. national.

1009. Plaintiff Jason Barlow is the stepfather of PFC Kreischer and a U.S. national. Mr. Barlow lived in the same household as PFC Kreischer for a substantial period and considered PFC Kreischer the functional equivalent of a biological son.

1010. Plaintiff Sage Saladin is the stepbrother of PFC Kreischer and a U.S. national. Mr. Saladin lived in the same household as PFC Kreischer for a substantial period and considered PFC Kreischer the functional equivalent of a biological brother.

1011. As a result of the July 29, 2019 Attack and PFC Kreischer's injuries and death, each member of the Kreischer Family has experienced severe mental anguish, emotional pain and suffering, and the loss of PFC Kreischer's society, companionship, and counsel.

1012. As a result of the July 29, 2019 Attack, PFC Kreischer was injured in his person and/or property. The Plaintiff members of the Kreischer Family are the survivors and/or heirs of PFC Kreischer and are entitled to recover for the damages PFC Kreischer sustained.

1013. **Specialist Michael Nance** served in Afghanistan as a member of the U.S. Army. SPC Nance was injured in the July 29, 2019 Attack. SPC Nance died on July 29, 2019, as a result of injuries sustained during the attack.

1014. SPC Nance was a U.S. national at the time of the attack and his death.

1015. Plaintiff ShuShawndra Gregoire is the mother of SPC Nance and a U.S. national.

1016. Plaintiff John Gregoire Jr. is the brother of Michael Nance and a U.S. national.

1017. Plaintiff John Gregoire Sr. is the stepfather of SPC Nance and a U.S. national. Mr. Gregoire lived in the same household as SPC Nance for a substantial period and considered SPC Nance the functional equivalent of a biological son.

1018. Plaintiff L.G., by and through her next friend John Gregoire Sr., is the minor stepsister of SPC Nance and a U.S. national. L.G. lived in the same household as SPC Nance for a substantial period and considered SPC Nance the functional equivalent of a biological brother.

1019. As a result of the July 29, 2019 Attack and SPC Nance's injuries and death, each member of the Nance Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Nance's society, companionship, and counsel.

1020. As a result of the July 29, 2019 Attack, SPC Nance was injured in his person and/or property. The Plaintiff members of the Nance Family are the survivors and/or heirs of SPC Nance and are entitled to recover for the damages SPC Nance sustained.

#### **5. The January 5, 2020 Complex Attack in Kenya (Harrison and Mayfield Families)**

1021. On January 5, 2020, al-Shabaab (a designated FTO at the time) committed a complex attack involving rocket propelled grenades, small arms fire, and mortars in Lamu, Kenya (the "January 5, 2020 Attack"). Al-Shabaab is a branch of, and received funding and logistical support from, al-Qaeda.

1022. The January 5, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, one of the victims of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1023. The January 5, 2020 Attack furthered the Axis Conspiracy by demonstrating the IRGC's (through IRGC proxies al-Qaeda and al-Shabaab, which was a branch of al-Qaeda) continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC's, Binance's,

and Zhao's ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC's ability to collect the highest prices for Axis Payments depended upon the IRGC's reputation for violence, which was bolstered by the January 5, 2020 Attack given its high-profile nature.

1024. **Dustin Harrison** was in Kenya as a civilian pilot working for the U.S. Department of Defense at the time of the attack. Dustin Harrison was injured in the January 5, 2020 Attack. Dustin Harrison died on January 5, 2020, as a result of injuries sustained during the attack.

1025. Dustin Harrison was a U.S. national at the time of the attack and his death.

1026. Plaintiff Hope Harrison is the widow of Dustin Harrison and a U.S. national.

1027. Plaintiff H.H., by and through her next friend Hope Harrison, is the minor daughter of Dustin Harrison. She is a U.S. national.

1028. Plaintiff Donna Harrison is the mother of Dustin Harrison and a U.S. national.

1029. Plaintiff Marlin Harrison is the brother of Dustin Harrison and a U.S. national.

1030. Plaintiff Heide Ryan is the sister of Dustin Harrison and a U.S. national.

1031. As a result of the January 5, 2020 Attack and Dustin Harrison's injuries and death, each member of the Harrison Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Dustin Harrison's society, companionship, and counsel.

1032. As a result of the January 5, 2020 Attack, Dustin Harrison was injured in his person and/or property. The Plaintiff members of the Harrison Family are the survivors and/or heirs of Dustin Harrison and are entitled to recover for the damages Dustin Harrison sustained.

1033. **Specialist Henry Mayfield Jr.** served in Kenya as a member of the U.S. Army. SPC Mayfield was injured in the January 5, 2020 Attack. SPC Mayfield died on January 5, 2020, as a result of injuries sustained during the attack.

1034. SPC Mayfield was a U.S. national at the time of the attack and his death.

1035. Plaintiff Henry Mayfield Sr. is the father of SPC Mayfield and a U.S. national.

1036. Plaintiff Danielle Davis is the sister of SPC Mayfield and a U.S. national.

1037. Plaintiff Taliyah Davis is the sister of SPC Mayfield and a U.S. national.

1038. Plaintiff Ronald Edwards is the brother of SPC Mayfield and a U.S. national.

1039. Plaintiff Nicholas Mayfield is the brother of SPC Mayfield and a U.S. national.

1040. Plaintiff Tyshauna White is the sister of SPC Mayfield and a U.S. national.

1041. Plaintiff Carmoneta Horton-Mayfield is the stepmother of SPC Mayfield and a U.S. national. Ms. Horton-Mayfield lived in the same household as SPC Mayfield for a substantial period and considered SPC Mayfield the functional equivalent of a biological son.

1042. Plaintiff Tyron Edwards is the stepbrother of SPC Mayfield and a U.S. national. Mr. Edwards lived in the same household as SPC Mayfield for a substantial period and considered SPC Mayfield the functional equivalent of a biological brother.

1043. Plaintiff Ciara Martin is the stepsister of SPC Mayfield and a U.S. national. Ms. Martin lived in the same household as SPC Mayfield for a substantial period and considered SPC Mayfield the functional equivalent of a biological brother.

1044. As a result of the January 5, 2020 Attack and SPC Mayfield's injuries and death, each member of the Mayfield Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SPC Mayfield's society, companionship, and counsel.

1045. As a result of the January 5, 2020 Attack, SPC Mayfield was injured in his person and/or property. The Plaintiff members of the Mayfield Family are the survivors and/or heirs of SPC Mayfield and are entitled to recover for the damages SPC Mayfield sustained.

**6. The January 31, 2020 Hostage-Taking Attack in Afghanistan (Frerichs Family)**

1046. On January 31, 2020, al-Qaeda and the Taliban, acting through its Haqqani Network (a designated FTO at the time of the attack), jointly committed a hostage-taking attack in Kabul Province, Afghanistan (the “January 31, 2020 Attack”).

1047. The January 31, 2020 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1048. The January 31, 2020 Attack furthered the Axis Conspiracy by, *inter alia*: (1) supplying co-Conspirators al-Qaeda and the Taliban (including its Haqqani Network) with a hostage whom the IRGC and its co-Conspirators, including Binance and Zhao, could potentially monetize through transactions involving the Binance exchange and the Nobitex Exchange; and (2) demonstrating the IRGC’s continuing ability (through IRGC proxies al-Qaeda and the Taliban) to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to the IRGC’s, Binance’s, and Zhao’s ability to maximize the benefit they derived from the Axis Conspiracy because the IRGC’s ability to collect the highest prices for Axis Payments depended upon its reputation for violence, which was bolstered by the January 31, 2020 Attack given its high-profile nature.

1049. **Mark Frerichs** was in Afghanistan working as the director of International Logistical Support at the time of the attack. The January 31, 2020 Attack severely wounded Mark Frerichs, who was held captive for over 31 months (more than 2 ½ years). He suffered from PTSD, anxiety, trouble sleeping, cold sweats and appetite issues.

1050. As a result of the January 31, 2020 Attack and his injuries, Mark Frerichs has experienced severe physical and emotional pain and suffering.

1051. Plaintiff Mark Frerichs was a U.S. national at the time of the attack and remains one today.

1052. Plaintiff Charlene Cakora is the sister of Mark Frerichs and a U.S. national.

1053. As a result of the January 31, 2020 Attack and Mark Frerichs's injuries, the Plaintiff members of the Frerichs family have experienced severe mental anguish as well as emotional pain and suffering.

**E. The ISIS Attacks in Niger, Syria, and Afghanistan**

**1. The October 4, 2017 Complex Attack in Niger (Black, Johnson, and Johnson Families)**

1054. On October 4, 2017, ISIS committed, planned, authorized a complex attack involving small arms fire, vehicle-mounted heavy machine guns, rocket propelled grenades, and mortars in Tongo Tongo, Niger that targeted American service members in Africa (the "October 4, 2017 Attack").

1055. The October 4, 2017 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1056. The October 4, 2017 Attack furthered the ISIS Conspiracy by demonstrating ISIS's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to ISIS's, Binance's, and Zhao's ability to maximize the benefit they derived from the ISIS Conspiracy because ISIS's need for the material support that Binance and Zhao agreed to supply depended entirely upon ISIS's propagation of violence. Violence created the demand and transaction activity that drove ISIS's, Binance's, and Zhao's ability to mutually benefit from their participation in the ISIS Conspiracy by maximizing ISIS's reputation for violence, which was bolstered by the October 4, 2017 Attack given its high-profile nature.

1057. **Staff Sergeant Bryan Black** served in Niger as a member of the U.S. Army. SSG Black was injured in the October 4, 2017 Attack. SSG Black died on October 4, 2017, as a result of injuries sustained during the attack.

1058. SSG Black was a U.S. national at the time of the attack and his death.

1059. Plaintiff Michelle Black is the widow of SSG Black and a U.S. national.

1060. Plaintiff Ezekiel Black is the son of SSG Black and a U.S. national.

1061. Plaintiff I.B., by and through his next friend Michelle Black, is the minor son of SSG Black. He is a U.S. national.

1062. Plaintiff Karen Black is the mother of SSG Black and a U.S. national.

1063. Plaintiff Henry Black is the father of SSG Black and a U.S. national.

1064. Plaintiff Jason Black is the brother of SSG Black and a U.S. national.

1065. As a result of the October 4, 2017 Attack and SSG Black's injuries and death, each member of the Black Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SSG Black's society, companionship, and counsel.

1066. As a result of the October 4, 2017 Attack, SSG Black was injured in his person and/or property. The Plaintiff members of the Black Family are the survivors and/or heirs of SSG Black and are entitled to recover for the damages SSG Black sustained.

1067. **Sergeant First Class Jeremiah Johnson** served in Niger as a member of the U.S. Army. SFC Johnson was injured in the October 4, 2017 Attack. SFC Johnson died on October 4, 2017, as a result of injuries sustained during the attack.

1068. SFC Johnson was a U.S. national at the time of the attack and his death.

1069. Plaintiff Crystal Johnson is the widow of SFC Johnson and a U.S. national.

1070. Plaintiff Addie Johnson is the daughter of SFC Johnson and a U.S. national.

1071. Plaintiff Elisa Johnson is the daughter of SFC Johnson and a U.S. national.

1072. Plaintiff John Johnson is the father of SFC Johnson and a U.S. national.

1073. Plaintiff Jennifer Johnson is the sister of SFC Johnson and a U.S. national.

1074. Plaintiff Jo-Anne Johnson is the stepmother of SFC Johnson and a U.S. national. Ms. Johnson lived in the same household as SFC Johnson for a substantial period and considered SFC Johnson the functional equivalent of a biological son.

1075. As a result of the October 4, 2017 Attack and SFC Johnson's injuries and death, each member of the Johnson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SFC Johnson's society, companionship, and counsel.

1076. As a result of the October 4, 2017 Attack, SFC Johnson was injured in his person and/or property. The Plaintiff members of the Johnson Family are the survivors and/or heirs of SFC Johnson and are entitled to recover for the damages SFC Johnson sustained.

1077. **Sergeant LaDavid Johnson** served in Niger as a member of the U.S. Army. SGT Johnson was injured in the October 4, 2017 Attack. SGT Johnson died on October 4, 2017, as a result of injuries sustained during the attack.

1078. SGT Johnson was a U.S. national at the time of the attack and his death.

1079. Plaintiff Myeshia Johnson is the widow of SGT Johnson and a U.S. national.

1080. Plaintiff Richshama Johnson is the sister of SGT Johnson and a U.S. national.

1081. As a result of the October 4, 2017 Attack and SGT Johnson's injuries and death, each member of the Johnson Family has experienced severe mental anguish, emotional pain and suffering, and the loss of SGT Johnson's society, companionship, and counsel.

1082. As a result of the October 4, 2017 Attack, SGT Johnson was injured in his person and/or property. The Plaintiff members of the Johnson Family are the survivors and/or heirs of SGT Johnson and are entitled to recover for the damages SGT Johnson sustained.

**2. The January 16, 2019 Suicide Bombing Attack in Syria (Farmer, Taher, and Wirtz Families)**

1083. On January 16, 2019, a suicide bomber deployed by ISIS detonated a suicide bomb at a restaurant in Manbij, Syria (the "January 16, 2019 Attack").

1084. The January 16, 2019 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the victim of this attack was a civilian not taking part in hostilities. Further, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1085. The January 16, 2019 Attack furthered the ISIS Conspiracy by demonstrating ISIS's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to ISIS's, Binance's,

and Zhao's ability to maximize the benefit they derived from the ISIS Conspiracy because ISIS's need for the material support that Binance and Zhao agreed to supply depended entirely upon ISIS's propagation of violence. Violence created the demand and transaction activity that drove ISIS's, Binance's, and Zhao's ability to mutually benefit from their participation in the ISIS Conspiracy by maximizing ISIS's reputation for violence, which was bolstered by the January 16, 2019 Attack given its high-profile nature.

1086. **Chief Warrant Officer 2 Jonathan Farmer** served in Syria as a member of the U.S. Army at the time of the attack. CW2 Farmer was injured in the January 16, 2019 Attack. CW2 Farmer died on January 16, 2019, as a result of injuries sustained during the attack.

1087. CW2 Farmer was a U.S. national at the time of the attack and his death.

1088. Plaintiff Tabitha Farmer is the widow of Jonathan Farmer and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of CW2 Farmer's estate.

1089. Plaintiff B.F., by and through her next friend Tabitha Farmer, is the minor daughter of CW2 Farmer. She is a U.S. national.

1090. Plaintiff D.F., by and through his next friend Tabitha Farmer, is the minor son of CW2 Farmer. He is a U.S. national.

1091. Plaintiff P.J.F., by and through his next friend Tabitha Farmer, is the minor son of CW2 Farmer. He is a U.S. national.

1092. Plaintiff P.F., by and through her next friend Tabitha Farmer, is the minor daughter of CW2 Farmer. She is a U.S. national.

1093. As a result of the January 16, 2019 Attack and CW2 Farmer's injuries and death, each member of the Farmer Family has experienced severe mental anguish, emotional pain and suffering, and the loss of CW2 Farmer's society, companionship, and counsel.

1094. As a result of the January 16, 2019 Attack, CW2 Farmer was injured in his person and/or property. The Plaintiff members of the Farmer Family are the survivors and/or heirs of CW2 Farmer and are entitled to recover for the damages CW2 Farmer sustained.

1095. **Ghadir Taher** was in Syria as a government interpreter working for U.S. Special Operations at the time of the attack. Ghadir Taher was injured in the January 16, 2019 Attack. Ghadir Taher died on January 16, 2019, as a result of injuries sustained during the attack.

1096. Ghadir Taher was a U.S. national at the time of the attack and her death.

1097. Plaintiff Amina Shaheen is the mother of Ghadir Taher and a U.S. national. She brings claims in both her personal capacity and representative capacity on behalf of Ghadir Taher's estate.

1098. Plaintiff Kawa Talabani is the stepfather of Ghadir Taher and a U.S. national. Mr. Talabani lived in the same household as Ghadir Taher for a substantial period and considered Ghadir Taher the functional equivalent of a biological daughter.

1099. As a result of the January 16, 2019 Attack and Ghadir Taher's injuries and death, each member of the Taher Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Ghadir Taher's society, companionship, and counsel.

1100. As a result of the January 16, 2019 Attack, Ghadir Taher was injured in her person and/or property. The Plaintiff members of the Taher Family are the survivors and/or heirs of Ghadir Taher and are entitled to recover for the damages Ghadir Taher sustained.

1101. **Scott Wirtz** was in Syria working for the Defense Intelligence Agency at the time of the attack. Scott Wirtz was injured in the January 16, 2019 Attack. Scott Wirtz died on January 16, 2019, as a result of injuries sustained during the attack.

1102. Scott Wirtz was a U.S. national at the time of the attack and his death.

1103. Plaintiff Sandra Wirtz is the mother of Scott Wirtz and a U.S. national.

1104. Plaintiff David Wirtz is the father of Scott Wirtz and a U.S. national.

1105. Plaintiff Frances Wirtz is the stepmother of Scott Wirtz and a U.S. national. Ms. Wirtz lived in the same household as Scott Wirtz for a substantial period and considered Scott Wirtz the functional equivalent of a biological son.

1106. As a result of the January 16, 2019 Attack and Scott Wirtz's injuries and death, each member of the Wirtz's Family has experienced severe mental anguish, emotional pain and suffering, and the loss of Scott Wirtz's society, companionship, and counsel.

1107. As a result of the January 16, 2019 Attack, Scott Wirtz was injured in his person and/or property. The Plaintiff members of the Wirtz Family are the survivors and/or heirs of Scott Wirtz and are entitled to recover for the damages Scott Wirtz sustained.

**3. The August 26, 2021 Suicide Bombing Attack in Afghanistan (Gee, Gretzon, and Schmitz Families)**

1108. On August 26, 2021, ISIS and the Haqqani Network jointly committed a suicide bombing attack in Kabul Province, Afghanistan for which ISIS played the role of triggerman and the Haqqani Network played the role of logistician (the "August 26, 2021 Attack").

1109. The August 26, 2021 Attack would have violated the laws of war if these terrorists were subject to them because, among other reasons, the terrorist(s) who committed the attack neither wore uniforms nor otherwise identified themselves as enemy combatants, and the attack indiscriminately placed civilians at risk.

1110. The August 26, 2021 Attack furthered the ISIS Conspiracy by demonstrating ISIS's continuing ability to credibly threaten and/or commit an act of terrorism resulting in the hostage-taking, murder, and/or maiming of a U.S. national, which was vital to ISIS's, Binance's, and Zhao's ability to maximize the benefit they derived from the ISIS Conspiracy because ISIS's need for the material support that Binance and Zhao agreed to supply depended entirely upon ISIS's propagation of violence. Violence created the demand and transaction activity that drove ISIS's, Binance's, and Zhao's ability to mutually benefit from their participation in the ISIS Conspiracy by maximizing ISIS's reputation for violence, which was bolstered by the August 26, 2021 Attack given its high-profile nature.

1111. **Sergeant Nicole Gee** served in Afghanistan as a member of the U.S. Marine Corps. Sgt Gee was injured in the August 26, 2021 Attack. Sgt Gee died on August 26, 2021, as a result of injuries sustained during the attack.

1112. Sgt Gee was a U.S. national at the time of the attack and her death.

1113. Plaintiff Richard Herrera is the father of Sgt Gee and a U.S. national.

1114. As a result of the August 26, 2021 Attack and Sgt Gee's injuries and death, Plaintiff Richard Herrera has experienced severe mental anguish, emotional pain and suffering, and the loss of Sgt Gee's society, companionship, and counsel.

1115. As a result of the August 26, 2021 Attack, Sgt Gee was injured in his person and/or property. Plaintiff Richard Herrera is the survivor and/or heir of Sgt Gee and is entitled to recover for the damages Sgt Gee sustained.

1116. **Corporal Michael Gretzon** served in Afghanistan as a member of the U.S. Marine Corps at the time of the attack. The August 26, 2021 Attack severely wounded Cpl

Gretzon, who suffered from TBI, PTSD, a left shoulder injury, hearing loss, complex regional pain syndrome, hand injuries, and wrist pain.

1117. As a result of the August 26, 2021 Attack and his injuries, Cpl Gretzon has experienced severe physical and emotional pain and suffering.

1118. Plaintiff Corporal Michael Gretzon was a U.S. national at the time of the attack and remains one today.

1119. Plaintiff Randi Gretzon is the wife of Cpl Gretzon and a U.S. national.

1120. As a result of the August 26, 2021 Attack and Cpl Gretzon's injuries, the Plaintiff members of the Gretzon Family have experienced severe mental anguish as well as emotional pain and suffering.

1121. **Lance Corporal Jared Schmitz** served in Afghanistan as a member of the U.S. Marine Corps. LCpl Schmitz was injured in the August 26, 2021 Attack. LCpl Schmitz died on August 26, 2021, as a result of injuries sustained during the attack.

1122. LCpl Schmitz was a U.S. national at the time of the attack and his death.

1123. Plaintiff Mark Schmitz is the father of LCpl Schmitz and a U.S. national.

1124. Plaintiff Suzanne Schmitz is the mother of LCpl Schmitz and a U.S. national.

1125. Plaintiff A.S., by and through her next friend Mark Schmitz, is the minor sister of LCpl Schmitz. She is a U.S. national.

1126. Plaintiff Cameron Schmitz is the brother of LCpl Schmitz and a U.S. national.

1127. Plaintiff E.S., by and through her next friend Mark Schmitz, is the minor sister of LCpl Schmitz. She is a U.S. national.

1128. Plaintiff Jaclyn Schmitz is the stepmother of LCpl Schmitz and a U.S. national. Ms. Schmitz lived in the same household as LCpl Schmitz for a substantial period and considered LCpl Schmitz the functional equivalent of a biological son.

1129. Plaintiff Travis Avenvili-Frkovic is the stepbrother of LCpl Schmitz and a U.S. national. Mr. Avenvili-Frkovic lived in the same household as LCpl Schmitz for a substantial period and considered LCpl Schmitz the functional equivalent of a biological brother.

1130. As a result of the August 26, 2021 Attack and LCpl Schmitz's injuries and death, each member of the Schmitz Family has experienced severe mental anguish, emotional pain and suffering, and the loss of LCpl Schmitz's society, companionship, and counsel.

1131. As a result of the August 26, 2021 Attack, LCpl Schmitz was injured in his person and/or property. The Plaintiff members of the Schmitz Family are the survivors and/or heirs of LCpl Schmitz and are entitled to recover for the damages LCpl Schmitz sustained.

**CLAIMS FOR RELIEF**

**COUNT ONE: VIOLATION OF THE ANTI-TERRORISM ACT**

**18 U.S.C. § 2333(d)(2)**

**[Secondary Liability; Aiding and Abetting; All Plaintiffs]**

1132. Plaintiffs incorporate their factual allegations above.

1133. To establish a claim for aiding and abetting under JASTA, 18 U.S.C. § 2333(d), Plaintiffs must show: (1) that they are U.S. nationals, or the estates, survivors, or heirs of U.S. nationals; (2) that they were injured by an act of “international terrorism,” as defined by 18 U.S.C. § 2331(1); (3) that the act of international terrorism was committed, planned, or authorized by a designated FTO; (4) that Defendants were generally aware that they were playing a role in an overall illegal or tortious activity from which the act of international terrorism was a foreseeable consequence; and (5) that Defendants knowingly provided substantial assistance.

1134. Every Plaintiff is a U.S. national, or the estate, survivor, or heir of a U.S. national.

1135. The terrorist attacks that injured Plaintiffs were acts of “international terrorism” because:

- a. the attacks involved violent and dangerous acts that violate the criminal laws of the United States and many States (or would if committed in the United States). In particular, each attack constituted one or more of murder, attempted murder, conspiracy to murder, kidnapping, and arson, in violation of state law; and the destruction of U.S. property by fire or explosive, conspiracy to murder in a foreign country, killing and attempted killing of U.S. employees performing official duties, hostage taking, damaging U.S. government property, killing U.S. nationals abroad, use of weapons of mass destruction, commission of acts of terrorism transcending national boundaries, and bombing places of public use, in violation of 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, and 2332f, respectively;

- b. the attacks, carried out by terrorists bent on expelling the United States and its allies from Iraq and the Middle East, appear to have been intended (i) to intimidate or coerce the civilian populations of Afghanistan, Iraq, Israel, the United States, and other nations, (ii) to influence the policy of the U.S., Israeli, Iraqi, and other governments by intimidation and coercion, and (iii) to affect the conduct of the U.S., Israeli, Iraqi, and other governments by mass destruction, assassination, and kidnapping; and
- c. the attacks occurred primarily outside the territorial jurisdiction of the United States.

1136. Each attack was committed, planned, or authorized by one or more FTOs. Every attack was committed by one or more of the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, or ISIS.

1137. Every attack, regardless of who committed it, was planned or authorized by an FTO; this includes Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or ISIS (each of which was designated as an FTO for the entire Relevant Period), and the IRGC (which was designated an FTO on April 15, 2019).

1138. Binance and Zhao were generally aware that they were playing a role in illegal activity, and that the terrorist attacks that injured Plaintiffs were a natural and foreseeable consequence of that activity.

1139. Binance and Zhao provided assistance knowingly and culpably, and not innocently or inadvertently. Binance and Changpeng Zhao did so with knowledge that they were aiding terrorist organizations carrying out attacks on Americans.

1140. Binance's and Zhao's assistance was substantial.

1141. Binance' and Zhao's assistance was pervasive and systemic. The assistance involved years of willful misconduct and tremendous sums of money that provided critically

important assistance to the foreign terrorist organizations that killed or injured Plaintiffs and their family members.

1142. As a result of Binance’s and Zhao’s liability under 18 U.S.C. § 2333(d), Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

**COUNT TWO: VIOLATION OF THE ANTI-TERRORISM ACT**  
**18 U.S.C. § 2333(d)(2)**

**[Conspiracy Liability; Ransom and Protection-Racket Predicates; Axis Victim Plaintiffs]<sup>23</sup>**

1143. Plaintiffs incorporate their factual allegations above.

1144. In or about 2017, Defendants entered a conspiracy led by the IRGC, in which the IRGC’s Axis of Resistance allies Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and the Taliban were also members, whose overall object was to maintain each such FTO’s ability to access the payments they received in connection with their hostage-taking, human trafficking, ransomware, and protection payment schemes (collectively, “Axis Payments”) in connection with such FTOs’ act of international terrorism in Iran, Iraq, Syria, Lebanon, Gaza, Afghanistan, and/or the United States. The Axis Payments were paid to such FTO through each co-Conspirator’s operation of, or willful participation in, an unlicensed money transmitting business (“MTB”) and each co-Conspirator’s operation of, or willful participation in, one or more of the other co-Conspirator’s MTB (hereinafter, the “Axis Conspiracy”).

1145. The Conspiracy began in or about 2017 when the IRGC and Hezbollah each joined the Conspiracy by agreeing to jointly exercise control of, and/or maintain a beneficial ownership or profit participation interest in, the illicit profits realized by IRGC front Nobitex

---

<sup>23</sup> “Axis Victim Plaintiffs” comprise every Plaintiff other than those Plaintiffs who were killed or injured in attacks committed by ISIS.

through the illicit transactions conducted on the Nobitex exchange that monetized the IRGC's and Hezbollah's acts of international terrorism targeting the United States.

1146. Nobitex was based in Iran and was the nominal owner of the Nobitex exchange. Nobitex was an IRGC front as was the Nobitex exchange, which the IRGC controlled and operated for the benefit of the IRGC (as a direct beneficiary) and Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and the Taliban (each, an indirect beneficiary of the IRGC's profits derived by the IRGC).

1147. From 2017 through the present, Binance has controlled the Binance exchange, doing so jointly with Zhao until at least November 2023.

1148. Binance and Zhao joined the Axis Conspiracy in or about 2017 when it agreed with the IRGC, through IRGC front Nobitex, and Zhao to operate the Binance exchange as an MTB alongside the Nobitex exchange and collaborate to break the law together through their operation of the MTB-to-MTB partnerships with the other Co-Conspirators and the Axis Payments relating thereto, and conducted transactions with the Nobitex exchange to transfer, convert, or conceal Axis Payments for which the IRGC was the direct beneficiary and Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and the Taliban were each an indirect beneficiary through the IRGC, given the IRGC's funding agreements with each such FTO pursuant to which the IRGC had a pattern and practice of earmarking a portion of all IRGC income to be transferred to the Qods Force, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and the Taliban, each of which the IRGC funded as a proxy.

1149. On information and belief, Kataib Hezbollah joined the Axis Conspiracy in or about 2017 or 2018 when it, *inter alia*, agreed to partner with the IRGC and Hezbollah such that Kataib Hezbollah, the IRGC, Hezbollah, Binance, and Zhao all derived mutual profit from such

FTOs' acts of international terrorism targeting the United States in Iraq, Syria, Iran, and/or the United States through subsequent transactions between the Binance exchange and the Nobitex exchange in which the IRGC, Hezbollah, Kataib Hezbollah, Binance, and Zhao all benefitted.

1150. On information and belief, Hamas joined the Axis Conspiracy in or about 2017 or 2018 when it, *inter alia*, agreed to partner with the IRGC and Hezbollah such that Hamas, the IRGC, Hezbollah, Binance, and Zhao all derived mutual profit from such FTOs' acts of international terrorism targeting the United States in Iraq, Syria, Iran, Israel, Gaza, and/or the United States through subsequent transactions between the Binance exchange and the Nobitex exchange in which the IRGC, Hezbollah, Hamas, Binance, and Zhao all benefitted.

1151. On information and belief, PIJ joined the Axis Conspiracy in or about 2017 or 2018 when it, *inter alia*, agreed to partner with the IRGC and Hezbollah such that PIJ, the IRGC, Hezbollah, Binance, and Zhao all derived mutual profit from such FTOs' acts of international terrorism targeting the United States in Iraq, Syria, Iran, Israel, Gaza, and/or the United States through subsequent transactions between the Binance exchange and the Nobitex exchange in which the IRGC, Hezbollah, PIJ, Binance, and Zhao all benefitted.

1152. On information and belief, al-Qaeda and the Taliban (acting through the Haqqani Network) joined the Axis Conspiracy in or about 2017 or 2018 when al-Qaeda and the Taliban (including its Haqqani Network), *inter alia*, simultaneously agreed to partner with the IRGC and Hezbollah such that al-Qaeda, the Taliban (including its Haqqani Network), the IRGC, Hezbollah, Binance, and Zhao all derived mutual profit from such FTOs' acts of international terrorism targeting the United States in Iraq, Syria, Iran, Afghanistan, Pakistan, and/or the United States through subsequent transactions between the Binance exchange and the Nobitex exchange in which the IRGC, Hezbollah, al-Qaeda, the Taliban, Binance, and Zhao all benefitted. On

information and belief, Haqqani Network operatives acting on behalf of dual-hatted al-Qaeda/Taliban terrorist Sirajuddin Haqqani jointly represented al-Qaeda and the Taliban as agent for both groups for purposes of the Conspiracy. Axis Victim Plaintiffs' belief is based upon public reports about Sirajuddin Haqqani's, and the Haqqani Network's, division of labor with al-Qaeda and the Taliban (of which the Haqqani Network was always a part) with respect to transnational matters relating to hostage-taking, kidnapping, human trafficking, and protection rackets.

1153. From 2017 through at least 2023, the IRGC and its Axis of Resistance allies built a thriving, multi-faceted, terrorist racket comprised of, *inter alia*: (1) hostage-taking and human trafficking offenses targeting U.S. nationals and dual U.S.-Iranian nationals; (2) human trafficking, sex trafficking, child sex trafficking, and child soldier offenses; (3) protection racket offenses; (4) ransomware offenses; and (5) narcotics trafficking offenses, on behalf of, or in partnership with, each of Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and the Taliban (including its Haqqani Network).

1154. Prior to the Conspiracy, the IRGC and its allies lacked a scalable, efficient, dark-money, financial solution avenue in which each co-Conspirator could foreseeably transfer or receive large 7- and 8-figure U.S.-dollar value Axis Payments. The Conspiracy solved that problem by enabling transfer of receipt of such funds through transactions leveraging both the Binance exchange and the Nobitex exchange for which both exchanges agreed with one another to operate as an MTB and break the law together through their operation of the MTB-to-MTB relationships with the other Co-Conspirators.

1155. Each member of the Conspiracy sought to—and did—mutually benefit from the Conspiracy, including the acts of international terrorism that furthered the Conspiracy.

1156. Each member of the Conspiracy sought to—and did—directly or indirectly profit from each Axis Payment made or received by any co-Conspirator from 2017 through at least November 2023.

1157. Each member of the Conspiracy sought to—and did—maintain an ability to reliably, securely, and rapidly, conduct any Axis Payment-related transfer or currency conversation that involved the Binance exchange and the Nobitex exchange through nonpublic means specifically intended to render ineffective any subsequent legal investigation concerning any such Axis Payment, including, but not limited to, an investigation concerning potential violation of the Antiterrorism Act, U.S. sanctions, AML/CFT, or other law by the United States or its allies, including by U.S. persons in the United States, Europe, and/or the Middle East.

1158. Each member of the conspiracy worked together to optimize their respective—and related—unlicensed MTB, through which they collected, laundered, stored, and re-deployed such payments and thereby promote the IRGC's, Hezbollah's, Kataib Hezbollah's, Hamas's, PIJ's, al-Qaeda's, and the Taliban's ransom and protection rackets within territories such FTOs controlled or contested, in violation of (among other statutes) 18 U.S.C. §§ 2339A, 2339B, and 2339C.

1159. The IRGC's, Hezbollah's, Kataib Hezbollah's, Hamas's, PIJ's, al-Qaeda's, and the Taliban's (including its Haqqani Network's) acts of international terrorism targeting U.S. citizens, including the attacks that killed and injured Axis Victim Plaintiffs, furthered the overall object of Defendants' conspiracy and were a foreseeable consequence of that conspiracy.

1160. Since October 8, 1997, the United States has designated Hezbollah as an FTO.

1161. Since October 8, 1997, the United States has designated Hamas as an FTO.

1162. Since October 8, 1997, the United States has designated PIJ as an FTO.

1163. Since October 8, 1999, the United States has designated al-Qaeda as an FTO.

1164. Since July 2, 2009, the United States has designated Kataib Hizballah as an FTO.

1165. Since September 19, 2012, the United States has designated the Haqqani Network as an FTO.

1166. Since April 15, 2019, the United States has designated the IRGC as an FTO.

1167. Binance and Zhao pleaded guilty in the United States District Court for the Southern District of New York to conspiring to conduct an unlicensed MTB, in violation of 18 U.S.C. §§ 1960(a) and 1960(b)(1)(B).

1168. The terrorist attacks that killed or injured Axis Victim Plaintiffs or their family members were acts of international terrorism committed by the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or the Taliban (including its Haqqani Network). They were violent acts and acts dangerous to human life that violated the criminal laws of the United States and many States, or would have violated those laws had they been committed within the territorial jurisdiction of the United States or of the States, including 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, 2339C(a)(1)(B), and 2339D.

1169. The terrorist attacks committed by the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or the Taliban (including its Haqqani Network) were intended to intimidate and coerce the civilian populations of the United States, Iraq, Iran, Lebanon, Israel, Afghanistan, and Pakistan; to influence through intimidation or coercion the policy of the government of the United States; and to affect the conduct of the government of the United States by means of mass destruction, assassination, and kidnapping.

1170. The terrorist attacks committed by the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or the Taliban (including its Haqqani Network) occurred primarily

outside the territorial jurisdiction of the United States and transcended national boundaries in terms of their means, locations, and intended audiences.

1171. Axis Victim Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by the IRGC, Hezbollah, Kataib Hezbollah, Hamas, PIJ, al-Qaeda, and/or the Taliban (including its Haqqani Network). Axis Victim Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

1172. As a result of Defendants' liability under 18 U.S.C. § 2333(d)(2), Axis Victim Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

**COUNT THREE: VIOLATION OF THE ANTI-TERRORISM ACT**  
**18 U.S.C. § 2333(d)(2)**  
**[Conspiracy Liability; Material-Support Predicate; ISIS Victim Plaintiffs]<sup>24</sup>**

1173. Plaintiffs incorporate their factual allegations above.

1174. In or about 2017, Binance and Zhao entered a conspiracy with ISIS with the overall goal of providing material support for ISIS in violation of 18 U.S.C. § 2339B (hereinafter, the "ISIS Conspiracy"). Defendants and ISIS also structured their transactions to disguise the nature of their support, in violation of 18 U.S.C. § 2339A. ISIS foreseeably attacked civilians, including U.S. civilians, throughout the ISIS Conspiracy, with Defendants' knowledge.

1175. The terrorist attacks that killed or injured ISIS Victim Plaintiffs or their family members were acts of international terrorism committed by ISIS. They were violent acts and acts

---

<sup>24</sup> "ISIS Victim Plaintiffs" exclusively comprise Plaintiffs who were killed or injured in attacks committed by ISIS.

dangerous to human life that violated the criminal laws of the United States and many States, or would have violated those laws had they been committed within the territorial jurisdiction of the United States or of the States, including 18 U.S.C. §§ 844(f)(2) or (3), 956(a)(1), 1114, 1203, 1361, 2332, 2332a, 2332b, 2339C(a)(1)(B), and 2339D.

1176. The terrorist attacks committed by ISIS were intended to intimidate and coerce the civilian populations of the United States, Afghanistan, Iraq, Syria, and Niger; to influence through intimidation or coercion the policy of the governments of the United States, Afghanistan, Iraq, Syria, and Niger; and to affect the conduct of the governments of United States, Afghanistan (until the Taliban seized power in August 2021), Iraq, Syria, and Niger by means of mass destruction, assassination, and kidnapping.

1177. The terrorist attacks committed by ISIS occurred primarily outside the territorial jurisdiction of the United States and transcended national boundaries in terms of their means, locations, and intended audiences.

1178. ISIS Victim Plaintiffs are U.S. nationals who were injured in their persons, properties, and/or businesses by reason of the terrorist attacks committed by ISIS. ISIS Victim Plaintiffs suffered economic, physical, and emotional injuries proximately caused by the attacks; are survivors and/or heirs of U.S. nationals who suffered such injuries; or both.

1179. As a result of Defendants' liability under 18 U.S.C. § 2333(d)(2), ISIS Victim Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

1180. Each member of the Conspiracy sought to—and did—mutually benefit from the Conspiracy, including the acts of international terrorism that furthered the Conspiracy.

1181. Each member of the Conspiracy sought to—and did—directly or indirectly profit from each ISIS-related transaction that flowed through the Binance exchange and supplied material support to ISIS.

1182. ISIS's acts of international terrorism targeting U.S. citizens, including the attacks that killed and injured ISIS Victim Plaintiffs, furthered the overall object of Defendants' conspiracy and were a foreseeable consequence of that conspiracy.

1183. Since December 17, 2004, the United States has designated ISIS as an FTO.<sup>25</sup>

1184. As a result of Defendants' liability under 18 U.S.C. § 2333(d)(2), ISIS Victim Plaintiffs are entitled to recover economic and non-economic damages, including solatium damages.

### **JURY DEMAND**

1185. In accordance with Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury on all issues so triable.

### **PRAYER FOR RELIEF**

1186. Wherefore, Plaintiffs pray this Court:

- a. Enter judgment against Defendants finding them jointly and severally liable under the Anti-Terrorism Act, 18 U.S.C. § 2333;
- b. Award Plaintiffs compensatory and punitive damages to the maximum extent permitted by law, and treble any compensatory damages awarded under the Anti-Terrorism Act pursuant to 18 U.S.C. § 2333(a);
- c. Award Plaintiffs their attorneys' fees and costs incurred in this action, pursuant to 18 U.S.C. § 2333(a);

---

<sup>25</sup> ISIS's original FTO designation took place in 2004 when what is today called ISIS was called al-Qaeda-in-Iraq; the latter turned into the former when ISIS split from al-Qaeda in 2014.

- d. Award Plaintiffs prejudgment interest; and
- e. Award Plaintiffs any such further relief the Court deems just and proper.

Dated: September 20, 2024

Respectfully submitted,

SPARACINO PLLC

/s/ Adam J. Goldstein

Adam J. Goldstein  
Ryan R. Sparacino (*pro hac vice* forthcoming)  
Geoffrey P. Eaton (*pro hac vice* forthcoming)  
Tejinder Singh  
Matthew J. Fisher (*pro hac vice* forthcoming)  
SPARACINO PLLC  
1920 L Street, NW, Suite 835  
Washington, D.C. 20036  
Tel: (202) 629-3530  
adam.goldstein@sparacinopllc.com  
ryan.sparacino@sparacinopllc.com  
geoff.eaton@sparacinopllc.com  
tejinder.singh@sparacinopllc.com  
matt.fisher@sparacinopllc.com

*Counsel for Plaintiffs*